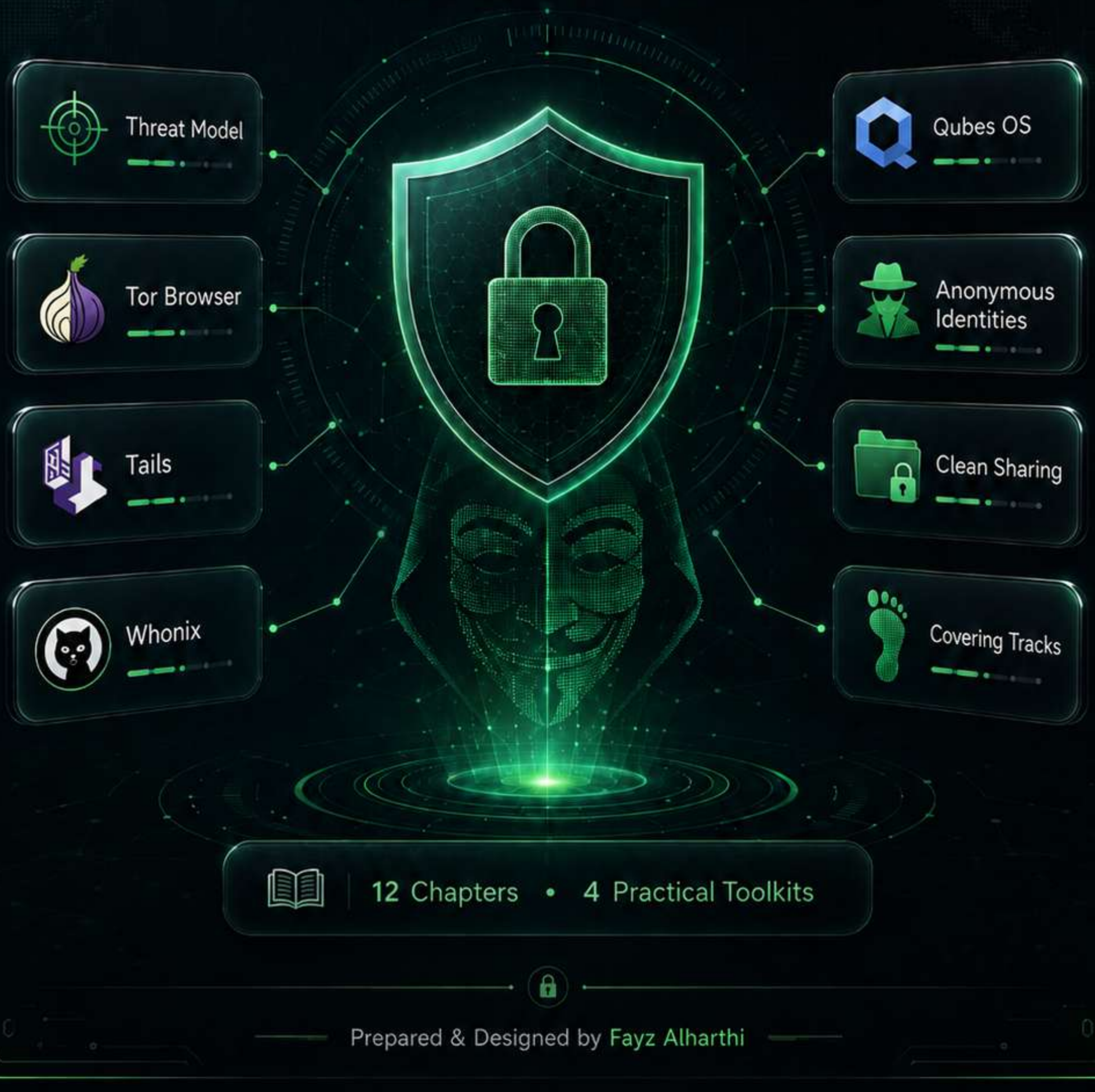
دليل الخصوصية الرقمية وإخفاء الهوية على الإنترنت

Digital Privacy & Online Anonymity Course

دليل عملي شامل للتصفح الآمن، العزل، بناء الهويات المجهولة، ومشاركة الملفات بأمان



12 Chapters • 4 Practical Toolkits

Prepared & Designed by Fayz Alharthi

الفصل الأول: المقدمة ونموذج التهديد

هذا الفصل يضع الأساس الكامل لبقية المقرر. الفكرة الرئيسية ليست فقط "إخفاء نفسك"، بل فهم ما هي **المجهولية Anonymity**، وما الفرق بينها وبين **الخصوصية Privacy**، وما حدود الحماية الواقعية، ومن هو الخصم الذي تحاول الحماية منه أصلًا.

4	3	2	1
محاور رئيسية	مستويات تهديد تقريبية	مفهومان أساسيان	قاعدة ذهبية

هدف الفصل

- فهم الغرض من الدليل: تحسين المجهولية على الإنترنت وليس فقط الخصوصية.
- استيعاب الفرق بين حماية النشاط، وحماية الهوية، وتقليل فرص الربط بينهما.
- التعرف على حدود الدليل: لا يعد بحماية مطلقة ضد الخصوم الأقوياء جدًا.
- بناء عقلية **Threat Model** قبل استخدام أي أداة مثل Tor أو VPN.

الفكرة المحورية: لا يوجد حل سحري واحد. النجاح يبدأ من معرفة خصمك، وما الذي يستطيع الوصول إليه، وما الذي تحاول حمايته بالضبط.

أهم أفكار البداية

Privacy
يعرف الآخرون من أنت، لكنهم لا يعرفون ماذا تفعل.

Anonymity
قد يعرف الآخرون ماذا يحدث، لكنهم لا يعرفون من الذي يقوم به.

Scope
الدليل يركز على المجهولية العملية، مع الاستفادة أيضًا من تقنيات الخصوصية والأمن.

Reality Check
الدليل ليس مناسبًا للحماية المطلقة ضد جهات استخباراتية ذات قدرات خارقة.

الفرق بين الخصوصية والمجهولية

الخصوصية Privacy

تركز على حماية **المحتوى** والبيانات الشخصية من الكشف أو المراقبة. قد تكون هويتك معروفة، لكن المطلوب هو عدم كشف نشاطك، ملفاتك، رسائلك، أو سلوكك.

من أنت معروف
ما تفعله غير واضح

المجهولية Anonymity

تركز على إخفاء **صلة الربط** بينك وبين النشاط. قد يكون النشاط ظاهرًا، لكن التحدي هو منع الوصول إلى الشخص الحقيقي خلفه.

النشاط قد يُرى
الهوية تبقى مجهولة

مهم: كثير من الناس يخلطون بين المصطلحين. استخدام اسم مستعار فقط لا يعني أنك أصبحت مجهولًا بالكامل.

Threat Model — نموذج التهديد

نموذج التهديد يعني تحديد: **من هو خصمك؟** ماذا يستطيع أن يرى؟ ما الأدوات التي يملكها؟ وما درجة الدقة المطلوبة منك؟ هذا التفكير يحدد إن كنت تحتاج فقط متصفح Tor، أو بيئة معزولة، أو أسلوب تشغيل كامل مختلف.

1 خصم منخفض القدرات

أشخاص عاديون، متطفلون، OSINT بسيط، منصات ومواقع تحتفظ بسجلات أساسية. هنا قد تكفي ممارسات جيدة وبعض أدوات الحماية الأولية.

2 خصم متوسط

جهات أكثر خبرة، تحليل ربط، متابعة السلوك، استغلال الأخطاء التشغيلية، ومراقبة الشبكة بشكل أوسع. هنا تبدأ الحاجة لأسلوب منظم وليس مجرد أداة واحدة.

3 خصم متقدم

جهات لديها وصول أوسع إلى السجلات أو قدرة أعلى على التحليل والتتبع والربط بين المؤشرات المختلفة. الحماية هنا أصعب وتحتاج انضباطًا عاليًا.

4 خصم شديد القوة

جهات استخباراتية أو خصوم عالميون بإمكانيات كبيرة جدًا. هذا الدليل يوضح أن الحماية الكاملة ضد هذا المستوى ليست مضمونة، ويجب معرفة حدودك بواقعية.

القاعدة الذهبية

قبل أن تفكر في الأدوات، اسأل نفسك:

- ما الذي أحاول إخفاءه؟
- ممن أحاول إخفاءه؟
- ما الذي سيحدث لو فشلت؟
- ما الميزانية والوقت والمهارة المتوفرة لدي؟

الخلاصة: الأداة المناسبة تأتي بعد تعريف المشكلة، وليس قبلها.

الاستخدامات المشروعة

- تجاوز الرقابة والقمع الإلكتروني.
- تقليل فرص التتبع والمضايقة والدكسنغ.
- الصحافة، النشاط الحقوقي، والإبلاغ الآمن.
- حماية الباحثين والأكاديميين وممارسي العمل الحساس.
- تعلم OPSEC وبناء عادات أفضل للخصوصية والأمن.

الفكرة هنا أن المجهولية ليست فقط "موضوع تقني"، بل قد تكون ضرورة حقيقية في بعض السياقات.

ما الذي لا يستهدفه الدليل

- إنشاء حسابات انتحال شخصية.
- الاستخدامات المسيئة أو الإجرامية أو غير الأخلاقية.
- الاعتماد عليه كضمان قانوني أو تقني مطلق.
- افتراض أن كل النصائح صالحة لكل دولة وكل تهديد بدون مراجعة.

يجب دائمًا التحقق من **القانون المحلي** وواقع التهديد الفعلي قبل تطبيق أي ممارسة.

Prerequisites & Limitations — المتطلبات والحدود

المتطلبات الأساسية

- فهم جيد للإنجليزية.
- حاسوب شخصي غير مشترك إن أمكن.
- صبر ووقت كافٍ للتعلم والتطبيق.
- استعداد لقراءة مراجع إضافية وعدم الاكتفاء بالسطحيات.

القيود الأساسية

- لا توجد حماية مثالية 100%.
- النجاح يعتمد على السلوك التشغيلي وليس الأدوات فقط.
- التهديدات تختلف من شخص لآخر.
- ما ينفع لمستخدم قد لا ينفع لآخر.

الخلاصة النهائية للفصل

الفصل الأول لا يعلّمك فقط "كيف تستخدم أدوات الحماية"، بل يجهز عقليتك للتعامل مع المجهولية بشكل صحيح. أهم نتيجة يجب أن تخرج بها هي أن **المجهولية ليست زرًا**، بل هي منظومة من قرارات، وسلوكيات، وأدوات، وحدود واقعية.

Takeaway: ابدأ دائمًا من فهم التهديد، ثم اختر الأدوات، ثم اضبط السلوك، ثم راقب نقاط التسريب المحتملة.

الفصل الثاني: كيف يمكن تتبعك على الإنترنت؟

هذا الفصل يشرح أهم الطرق التي قد تؤدي إلى كشف هويتك أو ربط نشاطك بك. التتبع لا يعتمد فقط على الكوكيز أو الحسابات الشخصية؛ بل قد يحدث عبر الشبكة، عنوان IP، طلبات DNS، الأجهزة المحيطة، الاتصالات اللاسلكية، وحتى تحليل حركة Tor و VPN.

6	3	2	1
مصادر تتبع رئيسية	طبقات شبكة مهمة	أخطاء شائعة	هدف: تقليل الربط

فكرة الفصل

الفكرة الأساسية هي أن كل اتصال أو جهاز أو سلوك قد يترك أثرًا. هذه الآثار قد لا تكشفك مباشرة وحدها، لكنها تصبح خطيرة عندما يتم **ربطها معًا**.

- عنوان IP قد يربط الاتصال بمزود الخدمة أو الموقع الجغرافي.
- طلبات DNS قد تكشف أسماء المواقع التي تزورها.
- Wi-Fi و Bluetooth قد يساعدان في تحديد موقعك أو تتبع حركتك.
- Rogue Access Points قد تراقب اتصالك في الأماكن العامة.
- Tor و VPN لا يمنعان كل أشكال التحليل والربط.

الخلاصة: الخطر الأكبر ليس في أثر واحد، بل في تجميع عدة آثار صغيرة لبناء صورة واضحة عنك.

Your IP Address

عنوان IP العام هو من أوضح طرق التتبع. غالبًا يتم منحه لك من مزود خدمة الإنترنت، وقد يتم الاحتفاظ بسجلات تربط العنوان بوقت وتاريخ استخدامه.

الخطر

إذا تسرب عنوان IP الأصلي، يمكن استخدامه لربط النشاط بمزود الخدمة، وربما بالهوية أو المنطقة أو الحسابات المستخدمة.

Location ISP Logs

التخفيف

استخدام Public Wi-Fi، أو Tor، أو VPN مدفوع بطريقة لا تربطه بهويتك، مع فهم أن هذه الحلول ليست مثالية.

VPN Tor

DNS Requests & IP Requests

DNS هو النظام الذي يحول أسماء المواقع مثل **example.com** إلى عناوين IP. المشكلة أن طلبات DNS قد تكشف أسماء المواقع التي تزورها، حتى لو كان الموقع نفسه يستخدم HTTPS.

العنصر	ما الذي قد يكشفه؟	ملاحظات مهمة
Plain DNS	اسم الموقع المطلوب بوضوح	قد يراه مزود الخدمة أو أي جهة على المسار
DoH / DoT	يشفّر طلب DNS	لا يحل كل المشكلة بسبب SNI وتحليل حركة الاتصال
SNI / ECH	قد يكشف اسم النطاق داخل TLS	ECH يحاول تقليل التسريب لكنه ليس مدعومًا دائمًا
IP Destination	عنوان الخادم الذي تتصل به	قد يكشف الموقع حتى لو تم إخفاء DNS

مهم: تشفير DNS وحده لا يعني أن نشاطك أصبح مجهولًا، لأن عنوان الخادم، SNI، وحجم/نمط الترافيك قد تكشف معلومات إضافية.

RFID Devices

أجهزة RFID تشمل البطاقات البنكية، بطاقات العمل، بطاقات المواصلات، المفاتيح الذكية، وبعض بطاقات الهوية أو الجوازات.

- لا تكشفك عادة عبر الإنترنت مباشرة.
- لكنها قد تساعد في التتبع الفيزيائي.
- وجودها معك في مكان حساس قد يترك أثرًا.

التخفيف يكون بتقليل حملها أو استخدام حافظات RFID blocking عند الحاجة.

Wi-Fi & Bluetooth Tracking

الأجهزة الحديثة تفحص الشبكات وأجهزة Bluetooth حولك. هذه الإشارات يمكن استخدامها في تحديد الموقع، بناء قواعد بيانات للأماكن، أو تتبع حركة المستخدمين داخل المتاجر والمباني.

1 Wi-Fi Scanning

الهاتف أو اللابتوب قد يبحث باستمرار عن الشبكات القريبة، مما يترك إشارات يمكن التقاطها وتحليلها.

2 Bluetooth Beacons

بعض الأجهزة ترسل إشارات Bluetooth يمكن استخدامها للقياس أو تحديد القرب أو تحليل الحركة.

3 Location Databases

شركات وأنظمة تشغيل قد تستخدم شبكات Wi-Fi و Bluetooth القريبة لتحسين تحديد الموقع حتى بدون GPS مباشر.

نقطة حساسة: إطفاء GPS لا يعني بالضرورة أن الموقع لم يعد قابلًا للاستنتاج.

Malicious / Rogue Wi-Fi Access Points

في الأماكن العامة قد يتم إنشاء نقطة وصول مزيفة تشبه الشبكة الأصلية. بعد الاتصال بها، يمكن للمهاجم مراقبة بعض أنماط الاتصال، محاولة التصيد، أو دفع المستخدم لتثبيت شهادة خبيثة.

- قد تنتحل اسم شبكة معروفة أو Captive Portal.
- قد تستخدم هجمات فصل الاتصال لإجبار الأجهزة على إعادة الاتصال.
- قد تحلل الترافيك حتى مع وجود HTTPS عبر metadata و traffic patterns.
- قد تستخدم في استهداف شخص داخل مكان مزدحم.

لا تثق بأي شبكة عامة لمجرد أن اسمها مألوف. الاسم وحده ليس دليلًا على الشرعية.

Tor / VPN Traffic Analysis

Tor و VPN يساعدان في إخفاء المصدر، لكنهما ليسا حلًا كاملًا. بعض الخصوم قد يحاولون استخدام تحليل التوقيت، الحجم، أو نمط الحركة لمحاولة الربط بين المصدر والوجهة.

Correlation Timing

مقارنة توقيت الاتصال عند المصدر والوجهة لاستنتاج العلاقة.

Traffic Fingerprinting

تحليل شكل الترافيك المشفر دون فك تشفيره.

Counting Attacks

مقارنة حجم البيانات المرسلة والمستقبلة خلال فترة معينة.

Exit/Entry Visibility

رؤية نقاط الدخول أو الخروج قد تساعد في الربط عند خصم قوي.

خريطة التتبع في هذا الفصل

مصدر التتبع	نوع الأثر	مستوى الخطورة	طريقة التخفيف العامة
IP Address	شبكي / جغرافي / سجلات مزود الخدمة	مرتفع	Tor, VPN مناسب، Public Wi-Fi مع حذر
DNS Requests	كشف أسماء المواقع	متوسط إلى مرتفع	DoH/DoT، Tor DNS، تقليل التسريبات
RFID	تتبع فيزيائي قريب	متوسط	عدم حمله، أو استخدام RFID blocking
Wi-Fi / Bluetooth	تحديد موقع / تتبع حركة	مرتفع في الأماكن العامة	إطفاء اللاسلكي، وضع الطيران، تقليل الأجهزة المحمولة
Rogue AP	تصيد / مراقبة / تحليل ترافيك	مرتفع	تجنب الشبكات العامة، VPN/Tor، عدم تثبيت شهادات غريبة
Tor/VPN Analysis	ربط عبر التوقيت أو الحجم أو النمط	يعتمد على الخصم	فهم الحدود، عدم خلط الهويات، تقليل الأنماط المتكررة

أخطاء شائعة

- الاعتقاد أن VPN وحده يجعل المستخدم مجهولًا بالكامل.
- إهمال DNS و SNI و metadata والتركيز فقط على عنوان IP.
- استخدام نفس الجهاز والحسابات والسلوك مع هوية مختلفة.
- الثقة في شبكات Wi-Fi عامة بدون تحقق.
- إبقاء Bluetooth/Wi-Fi يعملان أثناء نشاط حساس.

قواعد عملية من الفصل

- قلّل عدد الأجهزة التي تحملها عند أي نشاط حساس.
- لا تخلط بين الهوية الحقيقية والهوية المجهولة.
- افهم أن كل طبقة قد تسرب شيئًا مختلفًا.
- استخدم أدوات الحماية بناءً على Threat Model واضح.
- راقب الأنماط المتكررة؛ التكرار نفسه قد يصبح بصمة.

القاعدة الأهم: لا تعتمد على أداة واحدة. اعتمد على تقليل التسريبات عبر طبقات متعددة.

الخلاصة النهائية للفصل

هذا الفصل يوضح أن التتبع ليس شيئًا واحدًا، بل منظومة من المؤشرات: IP، DNS، الأجهزة اللاسلكية، نقاط الوصول المزيفة، وتحليل حركة الشبكة. حماية المجهولية تبدأ من فهم هذه المؤشرات، ثم تقليلها، ثم منع الربط بينها قدر الإمكان.

Takeaway: لا تسأل فقط "هل استخدمت Tor أو VPN؟"؛ اسأل: ما الآثار الأخرى التي ما زالت تكشفني أو تربط نشاطي بهويتي؟

الفصل الثالث: تسريبات الجهاز والهوية الرقمية

هذا الفصل يوضح أن الجهاز نفسه قد يكون مصدرًا قويًا للتتبع. ليست المشكلة في الاتصال فقط، بل في معرفات الجهاز، الهاتف، بطاقة SIM، عناوين MAC، Bluetooth، المعالج، وأنظمة التشغيل والتطبيقات التي قد ترسل بيانات تعريفية أو Telemetry تربط النشاط بالهوية.

7	2	3	1
مصادر تسريب	معرفات هاتف حرجة	طبقات جهاز	قاعدة: لا تخلط الأجهزة

فكرة الفصل

حتى لو أخفيت عنوان IP واستخدمت Tor أو VPN، قد يبقى الجهاز نفسه قابلًا للربط بك عبر معرفات ثابتة أو شبه ثابتة. هذه المعرفات قد تظهر في سجلات الشبكات، التطبيقات، أنظمة التشغيل، أو مزودي الخدمة.

- الهاتف قد يكشف IMEI و IMSI عبر الشبكات الخلوية.
- كرت الشبكة قد يترك MAC Address في بيئات معينة.
- Bluetooth قد يبث إشارات يمكن تتبعها.
- أنظمة التشغيل والتطبيقات قد ترسل Telemetry.
- الأجهزة الذكية قد تبث معلومات حتى عندما تبدو Offline.

الخلاصة: المجهولية ليست فقط إخفاء اتصالك؛ بل منع الجهاز نفسه من أن يصبح بصمتك الدائمة.

IMEI / IMSI / Phone Number

IMEI مرتبط بجهاز الهاتف نفسه، بينما **IMSI** مرتبط بشريحة الاتصال أو الاشتراك. عند اتصال الهاتف بالشبكة الخلوية، يمكن تسجيل هذه المعرفات وربطها بالموقع، الوقت، والشخص الذي اشترى الشريحة أو استخدم الجهاز.

الخطر

استخدام نفس الهاتف مع شرائح مختلفة قد يربط الهويات ببعضها. كذلك رقم الهاتف الحقيقي أصبح من أقوى معرفات الهوية الرقمية.

IMSI IMEI

التخفيف

لا تخلط بين هاتفك الحقيقي وأي نشاط حساس. الجهاز والشريحة والرقم يجب أن تكون منفصلة حسب نموذج التهديد.

Separation Burner Device

خريطة معرفات الجهاز

المعرف	مرتبط بماذا؟	كيف قد يسرّبك؟	التخفيف العام
IMEI	جهاز الهاتف	قد يربط الجهاز بسجلات شركة الاتصالات أو الشركة المصنعة	عدم استخدام نفس الهاتف لهويات مختلفة
IMSI	شريحة SIM والاشتراك	يرتبط غالبًا برقم الهاتف ومزود الخدمة	فصل الشريحة عن الهوية الحقيقية
MAC Address	كرت Wi-Fi أو Ethernet	قد يظهر للشبكات المحلية أو نقاط الوصول	MAC randomization وعدم الاتصال بشبكات مرتبطة بك
Bluetooth MAC	واجهة Bluetooth	قد يستخدم للتتبع القريب أو ربط الجهاز بالمكان	إطفاء Bluetooth عند عدم الحاجة
CPU / Firmware	المعالج والـ Management Engine	قد يمثل طبقة عميقة يصعب فحصها أو التحكم بها	اختيار عتاد مناسب، تحديثات، وتعطيل ما يمكن تعطيله
OS Telemetry	نظام التشغيل والتطبيقات	قد يرسل معرفات الجهاز أو نشاط المستخدم	إعدادات خصوصية، أنظمة منفصلة، وتقليل الخدمات

مهم: بعض المعرفات لا تظهر لك مباشرة، لكنها قد تكون موجودة في سجلات شركات الاتصالات، الشركات المصنعة، أنظمة التشغيل، أو التطبيقات.

MAC Address

عنوان MAC هو معرف لواجهة الشبكة مثل Wi-Fi أو Ethernet. قد تستخدمه الشبكات المحلية ونقاط الوصول للتعرف على الجهاز أو تتبع تكرار ظهوره.

- قد يظهر عند البحث عن الشبكات أو الاتصال بها.
- بعض الأنظمة تدعم MAC randomization.
- الاتصال بشبكات مرتبطة بك قد يربط الجهاز بهويتك.

استخدم العزل التشغيلي: جهاز منفصل، شبكات منفصلة، وسلوك منفصل.

Bluetooth MAC & Offline Tracking

بعض الأجهزة الحديثة يمكن أن تبث إشارات Bluetooth Low Energy حتى عندما تبدو غير متصلة بالإنترنت. الفكرة أن الأجهزة القريبة قد تلتقط هذه الإشارات وترسل الموقع أو الوجود إلى بعض أجهزة Samsung و MacBooks التي قد تستخدم BLE

1 BLE Broadcast

الجهاز قد يرسل إشارة قصيرة المدى يمكن أن تلتقطها أجهزة قريبة.

2 Nearby Devices

الأجهزة القريبة المتصلة بالإنترنت قد تعمل كوسيط لنقل وجود الجهاز أو موقعه.

3 Location Database

قد تُجمع هذه البيانات في قواعد بيانات تستخدم للعثور على الجهاز أو لأغراض تحليلية.

نقطة حساسة: لا تحمل أجهزة ذكية مرتبطة بهويتك أثناء نشاط حساس.

CPU & Firmware Risks

المعالجات الحديثة قد تحتوي على منصات إدارة داخلية مثل Intel Management Engine أو AMD Platform Security Processor. هذه الطبقات تعمل بمستوى منخفض جدًا داخل الجهاز، وقد تكون صعبة الفحص أو التعطيل بالنسبة للمستخدم العادي.

- تعمل في طبقة عميقة قريبة من العتاد.
- قد تملك وصولًا واسعًا لبعض وظائف الجهاز.
- ظهرت حول بعض هذه التقنيات مخاوف وثغرات أمنية عبر السنوات.
- تعطيلها ليس دائمًا ممكنًا أو سهلًا.

لا تعتمد على البرمجيات فقط إذا كان نموذج التهديد يتضمن خصمًا متقدمًا جدًا.

OS & App Telemetry

أنظمة التشغيل والتطبيقات قد تجمع وترسل بيانات تشخيصية أو تعريفية. أحيانًا تكون هذه البيانات مفيدة لتحسين الخدمة، لكنها قد تكون خطرة إذا ربطت الجهاز أو النشاط بهوية المستخدم.

Device IDs

معرفات الجهاز أو النظام قد تساعد في ربط الجلسات ببعضها.

Crash Reports

تقارير الأعطال قد تحتوي مسارات ملفات أو معلومات بيئة التشغيل.

Account Sync

مزامنة الحسابات قد تخلط بين الهوية الحقيقية والبيئة الحساسة.

App Permissions

بعض التطبيقات تطلب صلاحيات واسعة قد تكشف معرفات أو موقعًا أو جهات اتصال.

مستويات التسريب حسب الطبقة

الطبقة	أمثلة	ماذا تكشف؟	مستوى التحكم
Mobile Network	IMEI, IMSI, Cell Towers	الجهاز، الشريحة، الموقع التقريبي، وقت الاتصال	منخفض إلى متوسط
Local Network	Wi-Fi MAC, Ethernet MAC	وجود الجهاز في شبكة أو مكان معين	متوسط
Short Range	Bluetooth, BLE	قرب الجهاز من أجهزة أو أماكن معينة	متوسط
Hardware / Firmware	CPU Management Engines, BIOS/UEFI	طبقة منخفضة صعبة الفحص وقد تحتوي مخاطر عميقة	منخفض
Software Layer	OS Telemetry, Apps, Accounts	معرفات، استخدام، أخطاء، حسابات، مزامنة	متوسط إلى مرتفع

أخطاء شائعة

- استخدام نفس الهاتف الحقيقي في نشاط حساس.
- تغيير الشريحة فقط مع إبقاء نفس IMEI.
- إبقاء Bluetooth أو Wi-Fi يعملان بلا حاجة.
- تسجيل الدخول بحسابات شخصية داخل بيئة مجهولة.
- الاعتماد على VPN مع جهاز معروف ومربوط بهويتك.
- إهمال Telemetry الخاصة بالنظام والتطبيقات.

قواعد عملية من الفصل

- افصل بين الأجهزة حسب الهوية أو الاستخدام.
- لا تحمل هاتفك الحقيقي مع جهاز حساس في نفس المكان والوقت.
- أطفئ Wi-Fi و Bluetooth عند عدم الحاجة.
- لا تخلط الحسابات الشخصية مع البيئة المجهولة.
- استخدم نظامًا نظيفًا أو جهازًا مخصصًا عند الحاجة.
- راجع إعدادات Telemetry والصلاحيات.

القاعدة الأهم: الجهاز الذي عرفك سابقًا قد يعرفك لاحقًا، حتى لو غيّرت الشبكة أو الحساب.

الخلاصة النهائية للفصل

الفصل الثالث يوضح أن الجهاز قد يكون أخطر من الشبكة نفسها. فالمعرفات مثل IMEI وIMSI وBluetooth وMAC، إضافة إلى Telemetry وأنظمة التشغيل، قد تسمح بربط النشاط بالهوية. لذلك يجب بناء العزل من البداية: جهاز منفصل، حسابات منفصلة، شبكة منفصلة، وسلوك منفصل.

Takeaway: لا تسأل فقط "هل أخفيت عنوان IP؟". اسأل: هل الجهاز نفسه مرتبط بي أو بهويتي السابقة؟

الحزمة العملية الأولى: أدوات الخصوصية والعزل الأساسي

هذه الصفحة تجمع الجانب العملي من الفصول الثلاثة الأولى. الهدف هو تحويل المفاهيم النظرية إلى خطوات قابلة للتطبيق: اختبار التسريبات، تقليل التتبع، اختيار أدوات مناسبة، وفصل الجهاز والشبكة والهوية حسب نموذج التهديد.

5	8	3	1
مجموعات أدوات	اختبارات تسريب	طبقات عزل	Checklist نهائي

كيف تستخدم هذه الصفحة؟

هذه ليست قائمة شراء عشوائية. ابدأ أولًا بتحديد **Threat Model**: هل تريد حماية يومية بسيطة؟ أم عزل هوية كاملة؟ أم اختبار تسريبات جهاز وشبكة؟ بعد ذلك اختر الأدوات المناسبة فقط.

Daily Privacy

تقليل التتبع اليومي، تحسين إعدادات المتصفح، إيقاف Bluetooth/Wi-Fi عند عدم الحاجة.

Basic

Identity Separation

فصل الحسابات، الجهاز، الشبكة، وأسلوب الاستخدام لتقليل الربط بين الهويات.

OPSEC

Leak Testing

اختبار IP و DNS و WebRTC و Browser Fingerprint قبل الاعتماد على أي بيئة.

Testing

Physical Tracking Reduction

تقليل RFID و Bluetooth و Wi-Fi tracking، خصوصًا في الأماكن العامة.

Physical

RFID Blocking Tools

أدوات RFID blocking ليست حلًا سحريًا، لكنها مفيدة لتقليل التتبع أو القراءة القريبة لبعض البطاقات والأجهزة. استخدمها كطبقة حماية فيزيائية، وليس كبديل عن العزل التشغيلي.

Amazon Search: RFID Blocking Card
بطاقة توضع داخل المحفظة لتقليل قراءة RFID القريبة.

Amazon Search: RFID Blocking Wallet
محفظة مخصصة لتقليل قراءة البطاقات البنكية أو بطاقات الهوية RFID.

Amazon Search: Faraday Pouch for Phone
حقيبة عزل للهاتف لتقليل الإشارات اللاسلكية عند الحاجة.

تنبيه: لا تعتمد على وصف المنتج فقط. اختبره عمليًا إن أمكن، وتأكد من مراجعات موثوقة.

Phone & Device Isolation

الهاتف هو أكثر جهاز قابل لربطك بهويتك: رقم SIM، IMEI، حسابات، GPS، Wi-Fi، Bluetooth، صور، وجهات اتصال، ومزامنة سحابية. لذلك العزل يبدأ من الجهاز.

- **لا تحمل هاتفك الحقيقي أثناء نشاط حساس**
  وجود الهاتف معك قد يكفي لربط المكان والوقت بهويتك.
- **أفضل الجهاز عن الحسابات الشخصية**
  لا تدخل Gmail أو iCloud أو WhatsApp الشخصي داخل بيئة مجهولة.
- **عطّل Wi-Fi و Bluetooth عند عدم الحاجة**
  حتى البحث عن الشبكات قد يترك إشارات قابلة للتحليل.

Network & Browser Leak Tests

قبل الاعتماد على أي VPN أو Tor أو متصفح، اختبر التسريبات الأساسية. هذه الاختبارات لا تثبت أنك مجهول بالكامل، لكنها تساعدك في اكتشاف الأخطاء الواضحة.

الاختبار	الرابط	ماذا يفحص؟
Public IP	**whatismyip.com**	يعرض عنوان IP العام الظاهر للمواقع.
DNS Leak	**dnsleaktest.com**	يفحص هل DNS يخرج من مزود الخدمة أو جهة غير متوقعة.
Browser Leaks	**browserleaks.com**	يفحص WebRTC، Canvas، Fonts، WebGL، ومؤشرات بصمة المتصفح.
Tor Check	**check.torproject.org**	يتأكد هل اتصالك يخرج عبر Tor أم لا.
IP Reputation	**mxtoolbox.com**	يفحص هل عنوان IP موجود في قوائم حظر أو سمعة سيئة.
Device Fingerprint	**coveryourtracks.eff.org**	يفحص مدى تميز بصمة المتصفح بين المستخدمين.

قاعدة: الاختبار يجب أن يتم قبل النشاط، وبعد تغيير أي إعداد، وبعد تشغيل VPN/Tor.

Core Privacy Tools

هذه أدوات أساسية للفصل بين الهوية والشبكة والنظام. لا تستخدمها كلها عشوائيًا: اختر حسب نموذج التهديد.

Tor Browser
متصفح مبني لتقليل التتبع وإخفاء المصدر عبر شبكة Tor.

Tails OS
نظام Live يركز على الخصوصية ويعمل من USB دون ترك آثار واضحة على الجهاز.

Whonix
بيئة افتراضية تفصل بين Gateway و Workstation وتوجه الاتصال عبر Tor.

Qubes OS
نظام متقدم يعتمد على العزل بين البيئات والمهام المختلفة.

Password & Identity Tools

إدارة كلمات المرور والهوية جزء أساسي من العزل. إعادة استخدام كلمة مرور أو بريد أو اسم مستخدم قد يربط الهويات حتى لو كانت الشبكة محمية.

KeePassXC
مدير كلمات مرور محلي ومفتوح المصدر، مناسب لفصل قواعد بيانات الهويات.

Bitwarden
مدير كلمات مرور سحابي/ذاتي الاستضافة، مناسب للاستخدام اليومي المنظم.

SimpleLogin
خدمة Email aliases لتقليل ربط بريدك الحقيقي بالحسابات المختلفة.

addy.io
بديل Email aliasing يساعد في فصل الحسابات وتقليل التتبع بالبريد.

Quick Practical Workflow

هذا Workflow سريع قبل إنشاء بيئة أو تنفيذ نشاط حساس. الهدف ليس الوصول إلى حماية مطلقة، بل تقليل الأخطاء الواضحة التي تكشف الهوية.

المرحلة	الإجراء العملي	الهدف
قبل الاتصال	أطفئ الهاتف الحقيقي، Bluetooth، Wi-Fi auto-join	تقليل الربط الفيزيائي والمكاني
اختيار الشبكة	تجنب الشبكات الشخصية أو المرتبطة بك	تقليل ربط النشاط بمكانك أو ببيتك أو عملك
تشغيل البيئة	استخدم Tor Browser أو Tails أو Whonix حسب الحاجة	تقليل كشف IP وفصل النظام
اختبار التسريبات	افحص IP و DNS و WebRTC و Fingerprint	كشف الأخطاء قبل الاستخدام
الحسابات	لا تستخدم بريدك أو رقمك أو اسمك المعتاد	منع ربط الهوية الجديدة بالقديمة
بعد الانتهاء	أغلق الجلسة، لا تحفظ ملفات حساسة، وثّق الأخطاء	تقليل الآثار وتحسين OPSEC لاحقًا

Wireless Safety

- عطّل Wi-Fi auto-join.
- احذف الشبكات القديمة غير الضرورية.
- عطّل Bluetooth عند عدم الحاجة.
- لا تتصل بأي Captive Portal مشبوه.
- لا تثبت Certificates من شبكات عامة.

الشبكة العامة قد تكون مريحة حتى لو كان اسمها يبدو صحيحًا.

Device Fingerprint

- لا تغيّر إعدادات Tor Browser كثيرًا.
- لا تثبت إضافات كثيرة داخل المتصفح.
- لا تخلط نفس المتصفح بين هويتين.
- لا تستخدم نفس الخطوط والإعدادات دائمًا.
- اختبر Canvas / WebGL / Fonts leaks.

أحيانًا محاولة "تقوية الخصوصية" بشكل زائد تجعل بصمتك أكثر تميزًا.

Identity Separation

- اسم مستخدم مختلف.
- بريد مختلف.
- كلمة مرور مختلفة.
- جهاز أو VM منفصل.
- سلوك كتابة مختلف عند الحاجة.
- لا تربط الحسابات برقمك الحقيقي.

العزل الجيد يمنع الرابط، وليس فقط يخفي الاتصال.

Final OPSEC Checklist

- **هل عرّفت نموذج التهديد؟**
  من الخصم؟ ما قدرته؟ ما الذي تريد حمايته؟
- **هل جهازك مرتبط بهويتك الحقيقية؟**
  IMEI، حسابات، ملفات، صور، Telemetry، أو مزامنة سحابية.
- **هل اختبرت IP و DNS و WebRTC؟**
  لا تبدأ قبل التأكد من عدم وجود تسريب واضح.
- **هل أوقفت Bluetooth و Wi-Fi غير الضروري؟**
  قلل الإشارات القريبة التي قد تربطك بالمكان.
- **هل منعت خلط الهويات؟**
  لا تستخدم نفس البريد، الرقم، الاسم، الجهاز، أو نمط الاستخدام.

الخلاصة العملية: الأداة لا تكفي. العزل الحقيقي يتكون من جهاز منفصل، شبكة مناسبة، حسابات منفصلة، وسلوك لا يربط الهويات ببعضها.

الفصل الرابع: البيانات الشخصية، البصمة الرقمية والهندسة الاجتماعية

هذا الفصل يوضح أن كشف الهوية لا يحتاج دائمًا إلى اختراق تقني. أحيانًا يتم الربط من خلال معلومات صغيرة: صورة، موقع، أسلوب كتابة، قصة شخصية، بيانات وصفية، صوت، وجه، أو تفاعل اجتماعي يمكن استغلاله لبناء ملف OSINT يقود إلى الهوية الحقيقية.

6	3	2	1
مصادر كشف رئيسية	أنواع بصمات	مخاطر بشرية	قاعدة: لا تكشف السياق

فكرة الفصل

الخصوصية لا تنهار فقط بسبب IP أو جهاز. قد تنهار بسبب **معلومة شخصية صغيرة** تذكر مع الوقت: مدينة، جامعة، وقت نوم، لهجة، صورة، ذكرى، أسلوب كتابة، أو عادة رقمية.

- الصور والملفات قد تحتوي Metadata تكشف وقتًا أو موقعًا أو جهازًا.
- البصمة الرقمية قد تكشفك من أسلوب استخدامك وسلوكك.
- OSINT يجمع الأدلة الصغيرة لبناء صورة كبيرة.
- الوجه والصوت والقياسات الحيوية قد يربطك حتى خارج الإنترنت.
- الهندسة الاجتماعية تستهدف الإنسان قبل النظام.

الخلاصة: لا تشارك تفاصيل حقيقية داخل هوية مجهولة، حتى لو بدت التفاصيل بسيطة.

Metadata & Geolocation

البيانات الوصفية Metadata هي معلومات مخفية أو مرفقة بالملف، مثل وقت الإنشاء، نوع الجهاز، البرنامج المستخدم، الإحداثيات الجغرافية، أو اسم المستخدم داخل النظام.

الخطر

صورة واحدة قد تحتوي موقع التصوير، وقت التصوير، نوع الهاتف، أو بيانات أخرى تساعد في ربط الهوية المجهولة بالواقع.

Location EXIF

التخفيف

افحص الملفات قبل نشرها. أزل البيانات الوصفية. ولا تشارك صورًا أو مستندات خام من جهازك الحقيقي.

Redaction Metadata Removal

خريطة تسريبات البيانات الشخصية

المصدر	ما الذي قد يكشفه؟	مثال عملي	طريقة التخفيف
Metadata	وقت، موقع، جهاز، برنامج، اسم مستخدم	صورة EXIF فيها GPS أو مستند فيه اسم صاحب الجهاز	إزالة Metadata قبل النشر
Digital Footprint	الحسابات القديمة، التعليقات، الأسماء المتكررة	نفس username مستخدم في أكثر من منصة	فصل الهويات وعدم إعادة استخدام المعرفات
Online Behavior	أوقات النشاط، المواضيع، أسلوب التفاعل	نشاط دائم في توقيت مدينة معينة أو لهجة محددة	تقليل الأنماط المتكررة
OSINT Clues	تفاصيل حياة، ذكريات، جامعة، عمل، أماكن	ذكر قصة شخصية يمكن مطابقتها مع حساب حقيقي	عدم مشاركة تفاصيل واقعية قابلة للربط
Face / Voice	هوية بيومترية، مكان، وقت، أشخاص حولك	ظهورك في صورة شخص آخر أو فيديو عام	تجنب الظهور أو تشويه البيانات قبل النشر
Phishing	بيانات دخول، رموز تحقق، معلومات شخصية	رابط تسجيل دخول مزيف أو ملف مرفق خبيث	التحقق من الروابط وعدم مشاركة الرموز

Digital Fingerprint, Footprint & OSINT

البصمة الرقمية ليست شيئًا واحدًا. هي خليط من السلوك، الأسلوب، الحسابات، التوقيت، الاهتمامات، الأجهزة، والمعلومات المتراكمة. OSINT يستخدم هذه القطع الصغيرة للوصول إلى نتيجة أكبر.

1 Footprint — الأثر الرقمي

كل ما تركته سابقًا: حسابات، تعليقات، صور، أسماء مستخدمين، بريد، منشورات، أو أرشيفات.

2 Fingerprint — البصمة

خصائص تميزك: أسلوب كتابة، وقت نشاط، إعدادات متصفح، مواضيع متكررة، أو سلوك مشابه.

3 OSINT Correlation — الربط

جمع مؤشرات صغيرة من منصات مختلفة ومقارنتها للوصول إلى هوية أو تضييق دائرة البحث.

نقطة حساسة: لا تكتب تجاربك الحقيقية أو تفاصيل حياتك داخل هوية مجهولة؛ التراكم مع الوقت قد يكشفك.

Online Behavior

حتى بدون صور أو ملفات، السلوك وحده قد يكشفك. مثلًا: متى تدخل، كيف تكتب، ما المواضيع التي تركز عليها، وما الكلمات أو الأخطاء التي تكررها.

- أوقات النشاط اليومية.
- اللهجة أو المصطلحات المتكررة.
- نفس أسلوب الردود والنقاش.
- نفس الاهتمامات في أكثر من حساب.
- تكرار نفس الأخطاء الإملائية.

السلوك المتكرر قد يصبح معرفًا أقوى من الاسم.

Real Life Clues & OSINT

مشاركة تفاصيل من الحياة الواقعية داخل حساب مجهول قد تسمح لخصم متخبر ببناء ملف. وتحليل القرائن لتضييق دائرة البحث. مثال ذلك: قصص شخصية، أماكن، أحداث، جامعة، وظيفة. ذكريات متكررة، أو تفاصيل يمكن مطابقتها لاحقًا مع هوية حقيقية.

- لا تذكر الجامعة أو المدينة أو مكان العمل الحقيقي.
- لا تربط الأحداث بتواريخ دقيقة.
- لا تشارك صورًا من أماكن قريبة منك.
- لا تستخدم نفس النكات أو القصص في هويتين مختلفتين.
- لا تبني شخصية مجهولة على نسخة قريبة جدًا من شخصيتك الحقيقية.

Face, Voice, Biometrics & Pictures

الوجه والصوت والقياسات الحيوية أصبحت أدوات ربط قوية. ظهورك في صورة شخص آخر أو في مكان عام قد يضيف دقة. مثلًا: موقعًا تقريبيًا، أو سياقًا يمكن ربطه بهويتك. كما أن المنصات قد تستخدم تقنيات التعرف على الوجه لتنظيم الصور أو ربطها بحسابات وأشخاص.

Face Recognition

قد يربط صورك عبر منصات مختلفة حتى لو لم تنشرها بنفسك.

Voice Matching

الصوت واللهجة قد يكشفان منطقة أو هوية أو يربطان حسابات مختلفة.

Background Clues

الخلفية قد تكشف مكانك، منزلك، لوحة، انعكاسًا، أو جهازًا.

Timestamp & Location

الوقت والموقع قد يستنتجان حتى لو لم يكونا داخل Metadata.

Phishing & Social Engineering

الهندسة الاجتماعية تستهدف قرارات الإنسان. بدل كسر النظام، يحاول المهاجم جعلك تكشف المعلومات بنفسك: رابط مزيف، ملف مرفق، طلب تحقق، رسالة استعجال، أو انتحال شخصية.

الأسلوب	كيف يعمل؟	الإشارة التحذيرية	التصرف الصحيح
Fake Login	صفحة تشبه خدمة حقيقية لسرقة كلمة المرور	رابط غريب أو نطاق قريب من الأصلي	اكتب الرابط يدويًا أو استخدم Bookmark موثوق
Urgency	رسالة تضغط عليك لاتخاذ قرار سريع	"حسابك سيغلق خلال دقائق"	توقف وتحقق من مصدر الرسالة
Attachment Trap	ملف يحتوي Malware أو Metadata أو رابط داخلي	مرفق غير متوقع أو امتداد مزدوج	افتحه في بيئة معزولة أو لا تفتحه
Impersonation	انتحال شخص أو جهة موثوقة	أسلوب كلام غريب أو طلب غير معتاد	تحقق عبر قناة ثانية مستقلة

قاعدة: لا ترسل كلمات مرور، رموز 2FA، أو معلومات تعريفية بناءً على رسالة مفاجئة.

Pictures OPSEC

- أزل EXIF قبل النشر.
- راجع الخلفية والانعكاسات.
- لا تنشر صورًا من أماكن متكررة.
- انتبه للأوجاء، الشوارع، النوافذ، الأجهزة.
- لا تعتمد على blur ضعيف للمعلومات الحساسة.

الصورة قد تكشف أكثر مما يظهر في المقدمة.

Writing OPSEC

- لا تكرر نفس أسلوبك الحقيقي.
- لا تستخدم نفس العبارات المميزة.
- لا تذكر تجاربك الشخصية بدقة.
- لا تكشف المنطقة الزمنية من توقيت النشر.
- لا تستخدم نفس الأخطاء الإملائية دائمًا.

الأسلوب اللغوي قد يتحول إلى بصمة كتابة.

Social OPSEC

- لا تثق بالروابط المرسلة فجأة.
- لا تشارك رموز التحقق.
- لا تكشف معلومات عن بيتك أو جهازك.
- لا تدخل في محادثات شخصية غير ضرورية.
- تحقق من الهوية عبر قناة مستقلة.

أفضل دفاع ضد الهندسة الاجتماعية هو التوقف والتحقق.

Checklist الفصل الرابع

- [ ] **هل أزلت Metadata من الصور والملفات؟**
  خصوصًا EXIF، الموقع، اسم الجهاز، واسم المستخدم داخل المستند.
- [ ] **هل راجعت الخلفية قبل نشر أي صورة؟**
  انتبه للانعكاسات، اللوحات، الشوارع، الأجهزة، والنوافذ.
- [ ] **هل فصلت أسلوب الكتابة بين الهويات؟**
  لا تكرر نفس المصطلحات، التوقيت، القصص، أو الأخطاء.
- [ ] **هل تجنبت مشاركة تفاصيل حياتك الواقعية؟**
  لا تذكر الجامعة، العمل، المدينة، العائلة، أو الأحداث الدقيقة.
- [ ] **هل تحققت من الروابط والملفات قبل فتحها؟**
  الهندسة الاجتماعية تستهدفك أنت، وليس جهازك فقط.

الخلاصة النهائية للفصل

الفصل الرابع يوضح أن البيانات الشخصية والسلوك البشري قد يكونان أخطر من التسريبات التقنية. Metadata، الصور، الوجه، أسلوب الكتابة، والقصص الشخصية يمكن أن تتحول إلى أدلة OSINT تكشف الهوية. لذلك المجهولية تحتاج عزلًا معلوماتيًا وسلوكيًا، وليس عزلًا شكليًا فقط.

Takeaway: لا تسأل فقط "هل أخفيت الشبكة والجهاز؟" اسأل: هل المحتوى الذي أنشره يكشف من أنا؟

الفصل الخامس: مخاطر البرمجيات الخبيثة، الملفات والتشفير

هذا الفصل يشرح كيف يمكن أن تكون الملفات، التطبيقات، النسخ السحابية، المتصفح، والتشفير الضعيف مصادر خطيرة لكشف الهوية أو تسريب البيانات. الخطر لا يأتي فقط من الشبكة أو السلوك، بل من الملف الذي تفتحه، الصورة التي تنشرها، النسخة الاحتياطية التي ترفعها، أو خوارزمية التشفير التي تثق بها.

9	4	3	1
مصادر خطر رئيسية	أنواع تسريب ملفات	مخاطر تخزين	قاعدة: افحص قبل الثقة

فكرة الفصل

في الفصول السابقة ركزنا على الشبكة والجهاز والسلوك. هنا ننتقل إلى طبقة أخرى: **المحتوى والأدوات**. ملف PDF، صورة، تطبيق، USB، نسخة سحابية، أو إعداد تشفير خاطئ قد يكشف أكثر مما تتوقع.

- الملفات قد تحتوي Malware أو Metadata أو Watermarking.
- التطبيقات والخدمات قد تحتوي ثغرات أو تجمع بيانات أكثر من اللازم.
- USB قد يكون أداة هجوم وليس مجرد مساحة تخزين.
- Cloud Backup قد يكشف بيانات حساسة إن لم تكن مشفرة محليًا.
- التشفير السيئ أخطر من عدم التشفير لأنه يعطي إحساسًا زائفًا بالأمان.

الخلاصة: لا تتعامل مع الملفات والأدوات كأنها محايدة؛ كل ملف أو خدمة قد تكون مصدر تسريب أو نقطة ربط.

Malware in Files & Emails

الملفات والمرفقات قد تحتوي برمجيات خبيثة أو محتوى يستغل ثغرات في القارئ أو المتصفح أو نظام التشغيل. حتى ملف يبدو عاديًا مثل PDF أو Office document أو صورة قد يكون وسيلة لجمع معلومات أو تشغيل كود خبيث.

الخطر

فتح ملف غير موثوق قد يكشف عنوان IP، معلومات الجهاز، اسم المستخدم، أو يسمح بتنفيذ Malware داخل البيئة.

Malware | Exploit

التخفيف

افتح الملفات داخل بيئة معزولة، لا تستخدم جهازك الحقيقي، افحص الملفات، وقلل استخدام برامج قراءة معقدة عند عدم الحاجة.

Sandbox | Isolation

خريطة مخاطر الملفات والخدمات

المصدر	ما الخطر؟	مثال عملي	طريقة التخفيف
File Malware	تنفيذ كود، سرقة بيانات، كشف البيئة	PDF أو Office file يستغل ثغرة أو Macro	فتح داخل VM أو Sandbox وفحص الملف
App Exploits	ثغرات في التطبيقات والخدمات	متصفح أو قارئ ملفات غير محدث	تحديثات، عزل، تقليل الإضافات
Malicious USB	حقن أوامر، استغلال ثقة النظام، نقل Malware	USB يظهر كلوحة مفاتيح أو جهاز تخزين خبيث	عدم إدخال USB مجهول واستخدام جهاز اختبار منفصل
Metadata	كشف وقت، جهاز، برنامج، موقع، اسم مستخدم	صورة EXIF أو مستند فيه اسم صاحب الجهاز	إزالة Metadata قبل المشاركة
Watermarking	علامات مرئية أو مخفية لربط النسخة بالمستخدم	ملف PDF أو صورة تحمل معرفًا مخفيًا	استخدام مصادر عامة أو إزالة/إعادة إنشاء المحتوى بحذر
Cloud Backup	مزود الخدمة قد يصل للمحتوى أو يسلمه	رفع ملفات حساسة إلى Drive أو Dropbox	تشفير محلي قبل الرفع أو عدم استخدام

	لطرف ثالث	دون تشفير محلي	السحابة
Bad Cryptography	حماية وهمية أو قابلة للكسر	خوارزمية منزلية أو كلمة مرور ضعيفة	استخدام أدوات موثوقة وتجنب بناء تشفير خاص

Files, Documents, Pictures & Videos

الملفات ليست مجرد محتوى ظاهر. قد تحتوي بيانات وصفية، علامات مائية، طبقات مخفية، تاريخ تعديل، معلومات جهاز، أو أجزاء مرئية بشكل ضعيف يمكن استرجاعها أو تحليلها.

1 Properties & Metadata

قد تكشف اسم المستخدم، الجهاز، البرنامج المستخدم، وقت الإنشاء، الموقع، أو مسار الملف.

2 Watermarking

بعض الملفات تحتوي علامات ظاهرة أو مخفية تسمح بتتبع مصدر النسخة أو الشخص الذي سربها.

3 Pixelized or Blurred Information

الطمس الضعيف أو البكسلة قد لا تكون كافية؛ بعض المعلومات قد تُستنتج أو تستعاد جزئيًا.

نقطة حساسة: لا تعتمد على Blur أو Pixelation فقط لحجب معلومات حساسة. استخدم تغطية كاملة أو قصّ المنطقة من الأصل.

File Hygiene

قبل نشر أو إرسال أي ملف، تعامل معه كأنه يحمل آثارًا مخفية.

- افحص Metadata.
- أزل EXIF من الصور.
- لا تشارك ملفات أصلية من جهازك الحقيقي.
- لا تستخدم Blur ضعيف لإخفاء نصوص حساسة.
- افتح الملفات المشبوهة داخل VM.
- لا تثق في مرفقات غير متوقعة.

القاعدة العملية: صدّر نسخة نظيفة بدل مشاركة الأصل.

Malicious USB Devices

أجهزة USB ليست دائمًا مجرد ذاكرة تخزين. بعضها قد يتصرف كلوحة مفاتيح، كرت شبكة، أو جهاز إدخال ينفذ أوامر بسرعة. لذلك USB مجهول قد يكون أخطر من ملف مجهول.

- قد يحتوي Malware على مساحة التخزين.
- قد ينتحل Keyboard ويكتب أوامر تلقائيًا.
- قد يظهر كجهاز شبكة ويغير مسار الاتصال.
- قد يستغل ثقة النظام بالأجهزة الفيزيائية.

لا تدخل USB مجهول في جهازك الأساسي. استخدم جهاز اختبار منفصل أو بيئة معزولة.

Cloud Backups & Sync

النسخ السحابية والمزامنة قد تكون مفيدة، لكنها قد تكسر العزل. عند رفع ملفات حساسة دون تشفير محلي، قد يتمكن مزود الخدمة أو طرف ثالث من الوصول إليها أو تحليلها.

Content Access

بعض الخدمات قد تفحص المحتوى لتقديم البحث، الفهرسة، الحماية، أو الامتثال.

Account Linkage

استخدام حسابك الحقيقي للنسخ الاحتياطي قد يربط الملفات بك مباشرة.

Device Sync

المزامنة بين الأجهزة قد تنقل آثارًا من بيئة إلى أخرى.

Local Encryption

التخفيف الأفضل هو تشفير الملفات محليًا قبل رفعها أو تجنب الرفع.

Browser & Device Fingerprints

بصمة المتصفح والجهاز تتكون من خصائص كثيرة: نوع المتصفح، النظام، الخطوط، Canvas، WebGL، الإضافات، اللغة، المنطقة الزمنية، وحجم الشاشة. حتى لو خرجت من حسابك، قد تبقى البصمة نفسها وتربط جلسات مختلفة.

المؤشر	كيف يساهم في البصمة؟	المشكلة	التخفيف
Fonts	قائمة الخطوط تكشف النظام والبرامج المثبتة	قد تجعل جهازك مميزًا	استخدام Tor Browser أو بيئة موحدة
Canvas / WebGL	اختلافات الرسم تكشف خصائص الجهاز	بصمة شبه فريدة	تقليل JavaScript أو استخدام متصفح مقاوم للبصمة
Screen Size	حجم النافذة والشاشة جزء من البصمة	تغيير الحجم عشوائيًا قد يزيد التميز	استخدام إعدادات افتراضية موحدة
Extensions	الإضافات تكشف إعداداتك الخاصة	كل إضافة قد تضيف اختلافًا	لا تثبت إضافات كثيرة داخل بيئات مجهولة
Timezone / Language	تكشف منطقة أو نمط استخدام	تضييق دائرة البحث	فصل البيئة وعدم خلط الهويات

مهم: زيادة أدوات "مكافحة البصمة" بشكل عشوائي قد تجعل بصمتك أكثر ندرة. الأفضل استخدام بيئات موحدة مثل Tor Browser بإعداداته الافتراضية.

Local Data Leaks & Forensics

إذا وصل شخص إلى جهازك، قد يستطيع استخراج معلومات كثيرة حتى من جهاز مشفر أو مستخدم بحذر. الفحص الجنائي قد يبحث في الملفات المحذوفة، السجلات، الذاكرة، النسخ المؤقتة، التطبيقات، وسجلات المتصفح.

- ملفات مؤقتة وCache.
- سجلات التطبيقات والمتصفح.
- Thumbs, previews, recent files.
- بيانات محذوفة لكنها قابلة للاسترجاع.
- مزامنة سحابية مرتبطة بالجهاز.
- ذاكرة أو Swap أو Hibernation files.

التشفير مهم، لكنه لا يعوض سوء العزل أو ترك آثار داخل النظام أثناء التشغيل.

Bad Cryptography

التشفير الضعيف أو المصمم يدويًا قد يعطي إحساسًا زائفًا بالأمان. القاعدة المعروفة: **Don't roll your own crypto**. لا تخترع خوارزمية، ولا تستخدم مكتبات غير موثوقة، ولا تعتمد على كلمة مرور ضعيفة لحماية بيانات حساسة.

Weak Password

حتى التشفير القوي يضعف إذا كانت كلمة المرور سهلة التخمين.

Custom Crypto

الخوارزميات المنزلية غالبًا تنهار أمام التحليل الجاد.

Wrong Mode

استخدام خوارزمية صحيحة بطريقة خاطئة قد يكسر الحماية.

No Authentication

التشفير دون تحقق من السلامة قد يسمح بالتلاعب.

استخدم أدوات معروفة ومراجعة، وركّز على كلمات مرور قوية وإدارة مفاتيح صحيحة.

قواعد عملية للفصل الخامس

الحالة	التصرف الصحيح	السبب
استلام ملف مجهول	افتحه داخل VM أو Sandbox فقط	قد يحتوي Malware أو يستغل تطبيق القراءة
نشر صورة أو مستند	أزل Metadata وراجع الخلفية والمحتوى	قد يكشف الموقع، الجهاز، أو معلومات شخصية
إخفاء معلومات داخل صورة	استخدم تغطية كاملة أو قصّ المنطقة	الطمس الضعيف قد يُفك أو يُستنتج
رفع ملفات للسحابة	شفّر محليًا قبل الرفع	مزود الخدمة قد يصل للمحتوى أو Metadata
استخدام متصفح لهوية مجهولة	لا تضف إضافات كثيرة ولا تغير الإعدادات عشوائيًا	قد تجعل البصمة أكثر تميزًا
حماية ملفات حساسة	استخدم تشفيرًا معروفًا وكلمة مرور قوية	التشفير السيئ يعطي أمانًا وهميًا

أخطاء شائعة

- فتح مرفقات غير موثوقة على الجهاز الأساسي.
- نشر صور أصلية دون إزالة EXIF.
- استخدام Blur ضعيف لحجب بيانات حساسة.
- رفع ملفات حساسة للسحابة دون تشفير محلي.
- استخدام نفس المتصفح لهويات مختلفة.
- الثقة في VPN أو Cloud بمجرد وجود عبارة "No logs".

أفضل ممارسات

- افتح الملفات المشبوهة في VM.
- نظف Metadata قبل المشاركة.
- استخدم Password Manager.
- شفّر محليًا قبل النسخ السحابي.
- استخدم Tor Browser بإعداداته الافتراضية.
- حدّث التطبيقات وأنظمة التشغيل.

الأمان العملي يعني تقليل سطح الهجوم قبل حدوث المشكلة.

أسئلة فحص سريعة

- هل الملف من مصدر موثوق؟
- هل أحتاج فتحه على جهازي الأساسي؟
- هل يحتوي Metadata؟
- هل تم رفعه للسحابة؟
- هل المتصفح مميز بإضافات كثيرة؟
- هل كلمة المرور قوية وفريدة؟

إذا لم تعرف مصدر الملف، افترض أنه غير آمن.

Checklist الفصل الخامس

- ✓ **هل فتحت الملفات غير الموثوقة داخل بيئة معزولة؟**
  لا تستخدم جهازك الحقيقي لاختبار ملفات مجهولة أو مرفقات مشبوهة.
- ✓ **هل أزلت Metadata قبل نشر الصور والمستندات؟**
  راجع EXIF، اسم المستخدم، مسارات الملفات، ووقت الإنشاء.
- ✓ **هل استخدمت تغطية آمنة بدل Blur ضعيف؟**
  المعلومات المموهة بشكل ضعيف قد تُستنتج أو تُستعاد.
- ✓ **هل شفّرت البيانات محليًا قبل رفعها للسحابة؟**
  لا تثق في السحابة كمكان آمن للبيانات الحساسة دون تشفير من طرفك.
- ✓ **هل تتجنب بناء تشفير خاص بك؟**
  استخدم أدوات ومكتبات معروفة ومراجعة بدل حلول شخصية غير مختبرة.

الخلاصة النهائية للفصل

الفصل الخامس يوضح أن الملفات والخدمات قد تكسر المجهولية حتى لو كانت الشبكة والجهاز مضبوطين. Malware، Metadata، Watermarking، Cloud، Backups، Browser Fingerprints، Local Forensics، وBad Cryptography كلها طبقات خطر يجب التعامل معها بعقلية فحص وعزل.

Takeaway: لا تسأل فقط "هل اتصالي آمن؟"؛ اسأل: هل الملف، التطبيق، السحابة، والتشفير الذي أستخدمه آمنون فعلًا؟

Chapter 6 • General Preparations

الفصل السادس: التجهيزات العامة قبل بناء الهوية المجهولة

هذا الفصل يحوّل الفكرة من معرفة المخاطر إلى الاستعداد العملي. قبل اختيار Tor أو Tails أو Whonix أو Qubes، يجب تحديد الممرات، الوقت، الميزانية، المهارات، مستوى التخصص، وتجهيز الأساسيات مثل كلمات المرور، رقم هاتف منفصل، USB، وأماكن Wi-Fi عامة مناسبة.

8	4	3	1
تجهيزات رئيسية	قيود يجب حسابها	أدوات أساسية	قاعدة: خطط قبل التنفيذ

فكرة الفصل

التجهيزات العامة هي مرحلة بناء الأساس. لا تبدأ بإنشاء حسابات أو تشغيل أدوات قبل أن تعرف ما المسار المناسب لك، وما حدودك، وما الأشياء التي قد تربطك بهويتك الحقيقية.

- اختر Route مناسبة لمستوى التهديد.
- احسب الوقت والميزانية والمهارة المطلوبة.
- جهّز كلمات مرور قوية ومنفصلة.
- استخدم رقم هاتف منفصل إذا كان مطلوبًا.
- جهّز USB مناسبًا للمسارات العملية.
- حدد أماكن Wi-Fi عامة لا ترتبط بك مباشرة.

الخلاصة: الفشل غالبًا لا يأتي من الأداة، بل من التحضير السيئ والخلط بين الهويات.

Picking Your Route

اختيار المسار يعتمد على هدفك وتهديدك. شخص يريد تصفحًا خاصًا لا يحتاج نفس إعداد شخص يريد بناء هوية منفصلة طويلة المدى. لذلك يجب اختيار المسار قبل شراء الأجهزة أو إنشاء الحسابات.

خطأ شائع

البدء بأداة متقدمة دون فهم القيود، ثم استخدام حسابات حقيقية أو جهاز حقيقي داخلها.

Tool First

Weak OPSEC

التصرف الصحيح

حدد الهدف، الخصم، الميزانية، والوقت، ثم اختر المسار: Tor Browser، Tails، Whonix، أو Qubes.

Threat Model

Route Planning

خريطة اختيار المسار

المسار	مناسب لـ	المتطلبات	القيود
Tor Browser Route	تصفح مجهول أو تقليل تتبع أساسي	متصفح Tor وإعدادات سليمة	لا يعزل النظام بالكامل ولا يمنع كل أخطاء المستخدم
Tails Route	جلسات مؤقتة من USB مع تقليل الأثار المحلية	USB مناسب، معرفة إقلاع النظام، بيئة شبكة مناسبة	ليس مريحًا لكل الاستخدامات الطويلة أو اليومية
Whonix Route	عزل الشبكة داخل VMs وتوجيه الاتصال عبر Tor	VirtualBox، جهاز بمواصفات جيدة، قرص VMs	أعقد من Tor Browser ويحتاج ضبطًا وانضباطًا
Qubes Route	عزل متقدم بين المهام والهويات	جهاز متوافق، RAM كافية، خبرة تقنية أعلى	منحنى تعلم أعلى وقد لا يعمل على كل الأجهزة

مهم: المسار الأقوى ليس دائمًا الأفضل. المسار المناسب هو الذي تستطيع استخدامه بشكل صحيح ومستمر دون أخطاء تشغيلية.

Limits: Time, Budget, Skills & Adversary

قبل التنفيذ، قيّم القيود الواقعية. قد تحتاج أسابيع لإعداد بيئة قوية، وقد تحتاج جهازًا منفصلًا أو USB أو رقم هاتف منفصل أو أماكن Wi-Fi متعددة. كذلك المهارة التقنية تحدد هل تبدأ بطريق بسيط أو متقدم.

1 Timing Limitations

بعض الممرات تتطلب وقتًا للتعلم، الاختبار، التجهيز، وإنشاء عادات تشغيلية سليمة.

2 Budget / Material Limitations

الميزانية تحدد هل تستطيع استخدام جهاز منفصل، USB جيد، رقم منفصل، أو أدوات حماية فيزيائية.

3 Skills

كلما زاد تعقيد المسار، زادت الحاجة لفهم أنظمة التشغيل، الشبكات، الافتراضية، وإدارة الأخطاء.

4 Adversarial Considerations

خصم بسيط لا يتطلب نفس حماية خصم قادر على جمع سجلات شبكة أو تحليل سلوك طويل المدى.

Better Passwords

كلمات المرور هي أول تجهيز عملي. كل هوية تحتاج كلمات مرور منفصلة، قوية، وغير معاد استخدامها؛ إعادة استخدام كلمة مرور لو مرة واحدة قد يكسر كل الغرف.

Password Manager

استخدم KeePassXC أو مدير كلمات مرور موثوق لتنظيم الحسابات والهويات.

Unique Passwords

كل حساب يجب أن يملك كلمة مرور مختلفة بالكامل.

Passphrases

استخدم عبارات مرور طويلة بدل كلمات قصيرة سهلة التخمين.

Separate Databases

للهويات الحساسة، افصل قواعد بيانات كلمات المرور عن الاستخدام الشخصي.

كلمة مرور واحدة معاد استخدامها قد تربط حسابات كثيرة ببعضها.

USB Key

بعض الممرات تحتاج USB، خصوصًا Tails أو أدوات الإقلاع أو النقل الآمن. الملف يوضح بمقاليع USB عادية بحجم مناسب، مع تجنب الأجهزة "المشوهة ذاتيًا" المشكوك فيها.

- استخدم USB بسعة 16GB كحد أدنى.
- يفضل 32GB أو أكثر للراحة.
- احتفظ بواحد أو اثنين منفصلين.
- لا تستخدم USB مجهولي المصدر.
- لا تعتمد على USB self-encrypting عاميًا.

Anonymous Phone Number

كثير من المنصات تطلب رقم هاتف للتحقق. استخدام رقمك الحقيقي يربط الهوية الجديدة بك مباشرة. لذلك يناقش الفصل فكرة الحصول على رقم منفصل أو SIM منفصل قدر الإمكان، مع الانتباه للقوانين المحلية ومتطلبات التسجيل.

- لا تستخدم رقمك الشخصي لهوية مجهولة.
- افصل الهاتف، الشريحة، والحسابات عن هوياتك الحقيقية.
- تجنب الخدمات التي تطلب إثبات هوية إذا كان هدفك العزل.
- لا تتصل هاتفك الحقيقي مع الهاتف المنفصل في نفس النشاط.
- تحقق من قانونية شراء أو استخدام شرائح مسبقة الدفع في بلدك.

رقم الهاتف من أقوى روابط الهوية الرقمية؛ لا تتعامل معه كخدمة ثانوي.

Safe Public Wi-Fi Places

الفصل يوضح أن اختيار مكان Wi-Fi عام يحتاج وعيًا بالمحيط. ليس كل مكان عامًا مناسبًا. يجب تجنب الأماكن المرتبطة بك، الأماكن التي تتطلب دفعًا إلكترونيًا، أو الأماكن ذات كاميرات كثيرة أو نشاط تصوير عالٍ. يوصى بتحديد 3–5 أماكن مختلفة وعدم الاعتماد على مكان واحد.

المعيار	الأفضل	تجنّب
الارتباط بك	مكان لا علاقة له ببيتك أو عملك أو جامعتك	شبكة البيت، العمل، أو أماكن تتردد دائمًا
التسجيل	Wi-Fi بدون حساب أو تحقق هوية	شبكات تطلب رقمك أو بريدك الحقيقي
الدفع	تجنب الحاجة للدفع إن أمكن	شراء بكرت بنكي للحصول على كود Wi-Fi
الكاميرات	مكان أقل مراقبة وأقل تصويرًا	أماكن مليئة بـ CCTV أو تصوير الناس
التكرار	استخدم عدة أماكن بالتناوب	نفس المكان كل مرة

خريطة التجهيزات العملية

التجهيز	الهدف	الخطر عند تجاهله	الممارسة الأفضل
Threat Model	تحديد مستوى الحماية المطلوب	استخدام أدوات غير مناسبة أو زائدة	اكتب هدفك وخصمك وحدودك قبل التنفيذ
Route Selection	اختيار Tor / Tails / Whonix / Qubes	لاحيطة تقنية أو أخطاء تشغيلية	ابدأ بالمسار الذي تفهمه وتستطيع الالتزام به
Password Setup	منع ربط الحسابات بكلمات مرور معاد استخدامها	ربط عدة هويات ببعضها	مدير كلمات مرور وكلمات فريدة طويلة
Phone Number	تجاوز تحقق المنصات دون كشف رقمك الحقيقي	ربط مباشر بالهوية الشخصية	رقم منفصل وقانوني وغير مرتبط بحساباتك
USB Key	تشغيل أنظمة معزولة أو نقل أدوات بأمان	استخدام USB غير موثوق أو غير مناسب	USB مخروف المصدر وبسعة مناسبة
Public Wi-Fi Places	تقليل ربط الاتصال بمكانك الحقيقي	ربط النشاط بالبيت، العمل، أو كاميرات المكان	3–5 أماكن مختلفة، أقل ارتباطًا وتصويرًا

أخطاء شائعة

- بدء التنفيذ دون Threat Model واضح.
- استخدام رقم الهاتف الحقيقي.
- استخدام نفس كلمة المرور أو البريد.
- الاتصال من شبكة البيت أو العمل.
- استخدام نفس مكان Wi-Fi كل مرة.
- حمل الهاتف الحقيقي أثناء النشاط.

أفضل ممارسات

- اكتب خطة قصيرة قبل التنفيذ.
- ابدأ بمسار بسيط ثم تطور.
- جهز Password Manager منفصل.
- افصل الرقم والحسابات والجهاز.
- استخدم USB موثوقًا.
- اختر أماكن Wi-Fi متعددة.

التجهيز الجيد يقلل الأخطاء قبل أن تتحول إلى تسريبات.

أسئلة فحص سريعة

- هل المسار يناسب مهاراتي؟
- هل لدي وقت كافٍ للتجربة؟
- هل الهاتف، أو الرقم مرتبط بي؟
- هل الممكن فيه كاميرات كثيرة؟
- هل أستخدم حسابات شخصية؟
- هل يمكن تكرار نفس النمط وربطه بي؟

إذا كان الجواب غير واضح، لا تبدأ بعد.

Checklist الفصل السادس

- [ ] **هل حددت Threat Model واضحًا؟**
  من الخصم؟ ما قدرته؟ ما الذي تحميه؟ وما عواقب الفشل؟
- [ ] **هل اخترت المسار المناسب لمستواك؟**
  Tor Browser، Tails، Whonix، أو Qubes حسب الهدف والمهارة.
- [ ] **هل جهزت كلمات مرور منفصلة وقوية؟**
  لا تستخدم نفس كلمة المرور أو نفس البريد بين الهويات.
- [ ] **هل الرقم والهاتف منفصلان عن هويتك الحقيقية؟**
  رقمك الحقيقي يربط الحساب بك مباشرة.
- [ ] **هل حددت أماكن Wi-Fi مناسبة ومتعددة؟**
  تجنب البيت، العمل، الأماكن المرتبطة بك، أو الأماكن كثيرة التصوير.

الخلاصة النهائية للفصل

الفصل السادس هو مرحلة التخطيط قبل التنفيذ. تجاح المجهولية لا يعتمد فقط على اختيار Tor أو Tails أو Whonix، بل على تجهيز الهوية والأدوات بطريقة تمنع الربط منذ البداية. التخطيط السيئ يجعل أقوى الأدوات عديمة الفائدة.

Takeaway: لا تبدأ بإنشاء الحسابات أو تشغيل الأدوات قبل أن تكون الهاتف، الرقم، كلمات المرور، USB، ومكان الاتصال جاهزة ومنفصلة عن هويتك الحقيقية.

الحزمة العملية الثانية: تنظيف المحتوى، مقاومة التصيد وتجهيز الهوية

هذه الصفحة تجمع الجانب العملي من الفصول 4 إلى 6. الهدف هو تحويل مفاهيم Metadata وOSINT وSocial Engineering وFile Hygiene وGeneral Preparations إلى خطوات واضحة قبل نشر الملفات، فتح المرفقات، إنشاء الحسابات، أو استخدام شبكة عامة.

6	10	4	1
مجموعات أدوات	اختبارات عملية	Checklists	Workflow نهائي

هدف هذه الصفحة

بعد الفصول 4–6، لم يعد التركيز فقط على فهم المخاطر، بل على تطبيق إجراءات عملية: تنظيف الملفات قبل نشرها، فحص الروابط، فتح الملفات في بيئة معزولة، منع ربط السلوك بالهوية، وتجهيز كلمات المرور والرقم والـ USB والمكان قبل أي نشاط حساس.

Content OPSEC

تنظيف الصور والمستندات من Metadata ومراجعة الخلفيات والانعكاسات قبل النشر.

Metadata

Social OPSEC

تقليل القصص الشخصية، أسلوب الكتابة المتكرر، والبيانات التي تساعد OSINT.

OSINT

File Safety

فحص الملفات والمرفقات وفتحها في VM أو Sandbox بدل الجهاز الأساسي.

Malware

Preparation

تجهيز كلمات مرور، رقم منفصل، USB، وأماكن Wi-Fi مناسبة قبل التنفيذ.

Planning

Metadata Removal Tools

قبل مشاركة أي صورة أو مستند، افحص وأزل البيانات الوصفية Metadata قد تكشف الجهاز، وقت الإنشاء، الموقع، اسم المستخدم، البرنامج المستخدم، أو مسار الملف.

ExifTool
أداة قوية لفحص وإزالة Metadata من الصور والمستندات والملفات المتعددة.

MAT2 - Metadata Anonymisation Toolkit
أداة لإزالة Metadata من أنواع متعددة من الملفات، مفيدة في بيئات Linux.

VerExif
خدمة ويب لفحص وإزالة EXIF من الصور بسرعة. لا تستخدمها للصور الحساسة جدًا.

تنبيه: للملفات الحساسة، لا ترفعها لخدمة ويب. استخدم أداة محلية داخل بيئة معزولة.

Photo & Screenshot OPSEC

الصورة قد تكشف أكثر مما تقصده. ليست المشكلة فقط في EXIF: الخلفية، الانعكاسات، أسماء الملفات، علامات المكان، أو حتى نافذة صغيرة مفتوحة قد تكشف هوية أو موقعًا.

- **راجع الخلفية والانعكاسات**
  انتبه للمرايا، النوافذ، الشاشات، اللوحات، الشوارع، والأجهزة.
- **لا تستخدم Blur ضعيف**
  عتّم المعلومات الحساسة بمربع صلب أو قصّ الجزء بالكامل.
- **صدّر نسخة جديدة**
  لا تنشر الملف الأصلي القادم مباشرة من جهازك أو هاتفك.

Phishing & Social Engineering Toolkit

التصيد والهندسة الاجتماعية يستهدفان قرارك، وليس جهازك فقط. أي رابط أو مرفق أو رسالة استعجال يجب التعامل معها كاحتمال خطر حتى يتم التحقق منها.

الأداة / الاختبار	الرابط	الاستخدام	ملاحظة OPSEC
VirusTotal URL	virustotal.com	فحص الروابط المشبوهة	لا ترفع ملفات شديدة الحساسية لأنها قد تُشارك مع جهات أخرى
URLScan	urlscan.io	تحليل صفحة ورؤية الطلبات والنطاقات	قد تصبح الروابط المفحوصة عامة حسب الإعدادات
MXToolbox	mxtoolbox.com	فحص نطاقات، DNS، Blacklists	مفيد للتحقق من سمعة نطاق أو بريد
Have I Been Pwned	haveibeenpwned.com	فحص تسريب البريد	استخدمه لمعرفة إن كان بريدك قد ظهر في تسريبات
Google Safe Browsing	transparencyreport.google.com	فحص سمعة موقع	مؤشر مساعد وليس حكمًا نهائيًا

قاعدة: لا تدخل كلمة مرور أو رمز 2FA بعد الضغط على رابط وصل برسالة. افتح الموقع يدويًا.

Suspicious File Handling

أي ملف مجهول يجب فتحه داخل بيئة معزولة. لا تفتح PDF أو Office أو Archive أو Image مشبوه على جهازك الأساسي، خصوصًا إذا كان مرتبطًا بهويتك الحقيقية.

VirtualBox
بيئة افتراضية لاختبار الملفات بعيدًا عن النظام الأساسي.

VMware Workstation Player
خيار آخر لتشغيل أنظمة اختبار منفصلة.

Hybrid Analysis
خدمة تحليل ملفات وسلوك Malware. تجنب رفع ملفات شخصية أو سرية.

FileScan.IO
تحليل ملفات وروابط بشكل سلوكي. مفيد للملفات غير الحساسة.

Password & Identity Setup

بعد الفصول السابقة، أهم خطوة عملية هي منع إعادة استخدام نفس البريد، الرقم، كلمة المرور، أو اسم المستخدم بين الهويات. الربط قد يحدث من خطأ بسيط واحد.

KeePassXC
مدير كلمات مرور محلي مناسب لفصل قواعد بيانات الهويات المختلفة.

Bitwarden
مدير كلمات مرور عملي للاستخدام اليومي، ويمكن استخدامه داخل الاستضافة.

SimpleLogin
إنشاء بريد alias لتقليل ربط البريد الحقيقي بالحسابات.

addy.io
خدمة aliases للربط تساعد في فصل الحسابات وتخفيف التتبع.

استخدم قاعدة بيانات كلمات مرور منفصلة للهويات الحساسة بدل خلطها مع حساباتك الشخصية.

Practical Workflow: Before Publishing or Opening Anything

المرحلة	السؤال العملي	الإجراء الصحيح	الخطر إذا تجاهلتها
قبل نشر صورة	هل تحتوي EXIF أو خلفية كاشفة؟	إزالة Metadata ومراجعة الخلفية والانعكاسات	كشف موقع، جهاز، أو هوية
قبل نشر مستند	هل يحتوي اسم مستخدم أو معلومات مؤلف؟	استخدم MAT2 أو ExifTool وصدّر نسخة نظيفة	ربط الملف بجهازك أو اسمك
قبل فتح مرفق	هل المصدر موثوق ومتوقع؟	افتح داخل VM أو Sandbox فقط	Malware أو تسريب بيانات الجهاز
قبل الضغط على رابط	هل النطاق صحيح؟ هل الرسالة مستعجلة؟	افحص الرابط وافتح الموقع يدويًا	Phishing أو سرقة حساب
قبل إنشاء حساب	هل البريد/الرقم/الاسم مستخدم سابقًا؟	استخدم هوية منفصلة بالكامل	ربط الهوية الجديدة بالقديمة
قبل الاتصال بـ Wi-Fi	هل المكان مرتبط بك أو علیه بالكاميرات؟	اختر مكانًا أقل ارتباطًا وبدّل المواقع	ربط النشاط بالموقع الحقيقي

Writing OPSEC

- لا تكرر نفس أسلوبك الحقيقي.
- لا تذكر فضحتًا شخصية دقيقة.
- لا تكشف الجامعة أو المدينة أو العمل.
- لا تستخدم نفس النكات أو العبارات دائمًا.
- انتبه للتوقيت النشر والمنطقة الزمنية.
- لا تكرر نفس الأخطاء الإملائية المميزة.

أسلوب الكتابة قد يصبح بصمة شخصية مع الوقت.

Wi-Fi Place Checklist

- لا تستخدم شبكة البيت أو العمل.
- اختر 3–5 أماكن مختلفة.
- تجنب الأماكن المرتبطة بروتينك.
- تجنب أماكن كثيرة الكاميرات.
- لا تدفع ببطاقتك الشخصية للحصول على Wi-Fi.
- لا تستخدم نفس المكان في كل مرة.

لا تجعل الموقع نفسه يتحول إلى بصمة.

USB & Device Prep

- استخدم USB معروف المصدر.
- يفضل 32GB أو أكثر للأنظمة الحية.
- لا تدخل USB مجهول في جهازك الأساسي.
- جهّز USB منفصلًا لكل استخدام مهم.
- لا تخلط ملفاتك الشخصية مع بيئات مجهولة.
- اختبر الإقلاع قبل الحاجة الفعلية.

USB مجهول قد يكون جهاز هجوم، وليس مجرد ذاكرة.

Final Checklist: Chapters 4–6

- [ ] **هل نظّفت Metadata قبل النشر؟**
  افحص EXIF، اسم المستخدم، وقت الإنشاء، البرنامج، ومسارات الملفات.
- [ ] **هل راجعت الخلفية والمحتوى الظاهر؟**
  لا تنشر صورة فيها انعكاسات، موقع، لوحة، شاشة، أو تفاصيل شخصية.
- [ ] **هل فتحت الملفات المشبوهة داخل VM؟**
  لا تختبر المرفقات أو الملفات الغريبة على جهازك الأساسي.
- [ ] **هل تحققت من الروابط قبل إدخال أي بيانات؟**
  افتح المواقع يدويًا ولا ترسل كلمات مرور أو رموز 2FA من رابط مفاجئ.
- [ ] **هل جهزت الهوية قبل الاستخدام؟**
  بريد منفصل، رقم منفصل، كلمات مرور منفصلة، جهاز أو بيئة منفصلة.
- [ ] **هل اخترت مكان اتصال غير مرتبط بك؟**
  تجنب البيت، العمل، الجامعة، الأماكن الروتينية، وكاميرات كثيرة.

الخلاصة العملية: قبل أن تنشر، تفتح، تضغط، أو تنشئ حسابًا، اسأل: هل هذا المحتوى أو المكان أو السلوك يمكن أن يربطني بهويتي الحقيقية؟

الفصل السابع: مسار Tor Browser وTails

هذا الفصل يبدأ أول مسارين عمليين بعد مرحلة التجهيز: استخدام Tor Browser كخيار سريع وبسيط، ثم استخدام Tails كنظام حي يعمل من USB لتقليل الآثار المحلية. الفكرة الأساسية: اختيار المسار المناسب حسب الوقت، المهارة، الجهاز، ونموذج التهديد.

2	4	1	1
مسارات رئيسية	منصات Tor	نظام Live USB	قاعدة: لا تعدّل بلا فهم

فكرة الفصل

بعد تجهيز كلمات المرور والرقم والـ USB وتمكين الاتصال، يبدأ التطبيق العملي. Tor Browser مناسب للبداية السريعة، بينما Tails مناسب عندما تريد جلسة مؤقتة تقلل الآثار على الجهاز المستخدم.

- Tor Browser يوجه التصفح عبر شبكة Tor.
- Tails يعمل من USB كنظام Live مستقل.
- Tor ليس حلًا سحريًا إذا أخطأ المستخدم في السلوك.
- Tails يقلل الآثار المحلية لكنه لا يمنع كل أنواع التتبع.
- إعدادات Tor الافتراضية عالية أفضل من التعديل العشوائي.

الخلاصة: Tor وTails أدوات قوية، لكن قيمتها الحقيقية تظهر فقط عندما تستخدمها مع عزل الهوية والسلوك والجهاز.

Tor Browser Route

مسار Tor Browser هو الأبسط والأسرع للبدء. يناسب من لديه وقت محدود أو مهارات تقنية قليلة، ويريد تقليل تتبع الشبكة والتصفح دون كشف IP الأصلي للمواقع.

متى تستخدمه؟

عندما تحتاج حلًا سريعًا للتصفح، أو عندما لا تستطيع تجهيز USB أو جهاز منفصل، أو عندما يكون مستوى التهديد منخفضًا إلى متوسط.

Fast Start

Simple Route

حدوده

لا يعزل نظام التشغيل بالكامل، ولا يمنعك من كشف نفسك إذا سجلت الدخول بحسابات الحقيقي أو حملت ملفات خطرة.

No Full Isolation

User Mistakes

مقارنة Tor Browser وTails

العنصر	Tor Browser	Tails	ملاحظة مهمة
طريقة التشغيل	تطبيق يعمل داخل نظامك الحالي	نظام Live يعمل من USB	Tails يعزل الجلسة أكثر من مجرد متصفح
سهولة الاستخدام	أسهل وأسرع	يحتاج USB وإقلاع من الجهاز	Tor Browser مناسب كبداية
الآثار المحلية	قد تبقى آثار داخل النظام	مصمم لتقليل الآثار بعد الإغلاق	لا تعتمد على ذلك كضمان مطلق
العزل	يعزل التصفح فقط بدرجة محدودة	يعزل جلسة كاملة داخل نظام مؤقت	كلاهما يحتاج سلوك OPSEC صحيح
المهارة المطلوبة	منخفضة	متوسطة نسبيًا	Tails يحتاج BIOS/Boot وUSB
الاستخدام الطويل	أسهل يوميًا	أقل راحة للاستخدام الطويل	حسب الهدف ونموذج التهديد

Tor Browser على الأنظمة المختلفة

يقسم Tor Browser حسب المنصة: Windows وLinux وmacOS، ثم Android، ثم iOS. الفكرة أن التجربة ليست متساوية دائمًا؛ بعض المنصات أفضل دعمًا وأقرب للتجربة الرسمية من غيرها.

1 Windows / Linux / macOS

الاستخدام المكتبي هو المسار الأكثر مباشرة. حمّل Tor Browser من المصدر الرسمي، ولا تثبّت إضافات أو تغيّر إعدادات كثيرة بدون سبب واضح.

2 Android

يمكن استخدام Tor Browser على Android، لكن الهاتف بطبيعته يحتوي طبقات تتبع كثيرة: رقم SIM، حسابات، Telemetry، Wi-Fi، Bluetooth، وGPS.

3 iOS

iOS يفرض قيودًا على محركات المتصفح وطريقة عمل التطبيقات، لذلك التجربة لا تكون مساوية دائمًا لتجربة Tor Browser المكتبية.

4 Important Warning

استخدام Tor لا يحميك من تسجيل الدخول بحساب حقيقي، تنزيل ملف يكشفك، مشاركة معلومات شخصية، أو استخدام جهاز مرتبط بك.

مهم: لا تجعل Tor Browser فريدًا بكثرة الإضافات والتعديلات. الإعدادات الافتراضية تساعد على جعل المستخدمين أكثر تشابهًا.

أخطاء Tor الشائعة

- تسجيل الدخول بحساب شخصي داخل Tor.
- استخدام نفس اسم المستخدم في هويتين.
- تثبيت إضافات كثيرة داخل Tor Browser.
- تغيير حجم النافذة أو الإعدادات بلا حاجة.
- تنزيل وفتح ملفات على النظام الحقيقي.
- الاعتقاد أن Tor يمنع كل أشكال التتبع.

Tor يحمي جزءًا من الشبكة، لكنه لا يصلح أخطاء الهوية والسلوك.

The Tails Route

Tails هو نظام Live يعمل عادة من USB. الهدف منه توفير بيئة مؤقتة تركز على الخصوصية، وتقلل ترك الآثار المحلية على الجهاز بعد الإغلاق. يناسب من يحتاج أكثر من مجرد متصفح داخل نظامه الشخصي.

- يعمل من USB بدون تثبيت دائم على الجهاز.
- يوجه الاتصال عادة عبر Tor.
- مصمم لتقليل الآثار المحلية بعد انتهاء الجلسة.
- مفيد عند استخدام جهاز غير مخصص بالكامل.
- يحتاج اختيار الإقلاع والتوافق قبل الاعتماد عليه.

Tails مناسب كخطوة عملية بعد فهم Tor Browser وتجهيز USB ومكان الاتصال.

Tor Settings on Tails

داخل Tails، Tor Browser يأتي ضمن بيئة مصممة لتقليل التسريبات. الهدف ليس تعديل كل شيء، بل استخدام الإعدادات بعقلانية. وفهم أن أي تغيير غير ضروري قد يزيد البصمة أو يسبب تسريبًا.

Default Settings

الإعدادات الافتراضية تساعد على تقليل التمييز بين المستخدمين.

Security Level

رفع مستوى الحماية يقلل بعض المخاطر لكنه قد يكسر بعض المواقع.

No Personal Accounts

لا تدخل بحساباتك الحقيقية داخل جلسة تريدها مجهولة.

Session Discipline

عامل كل جلسة كهوية منفصلة ولا تخلط الملفات أو الحسابات.

القاعدة: لا تغيّر إعدادات Tor/Tails إلا إذا كنت تعرف بالضبط لماذا تفعل ذلك وما أثره على البصمة.

خريطة الاستخدام العملي

السيناريو	المسار الأنسب	لماذا؟	انتبه إلى
تصفح سريع مع وقت محدود	Tor Browser	أسهل وأسرع في الإعداد	لا تستخدم حساباتك الشخصية
استخدام جهاز واحد ولا تريد ترك آثار واضحة	Tails	يعمل من USB ويقلل الآثار المحلية	اختبر الإقلاع والتوافق مسبقًا
هاتف فقط ولا يوجد لابتوب	Tor Browser على Android بحذر	حل متاح لكنه أقل عزلًا بسبب طبيعة الهاتف	الهاتف مليء ببصمات وتتبعات
بيئة عامة أو غير موثوقة	Tails عالية أفضل	جلسة مؤقتة أكثر فصلًا عن النظام المثبت	الشبكة والكاميرات والسلوك ما زالت عوامل خطر
حاجة لعزل متقدم وطويل المدى	انتقل لاحقًا إلى Whonix/ Qubes	Tor/Tails قد لا يكفيان لكل حالات العزل الطويل	الفصول القادمة تغطي ذلك

متى لا يكفي CH7؟

- إذا كنت تحتاج عزل VMs دائم.
- إذا كنت تدير عدة هويات منفصلة طويلًا.
- إذا كان جهازك الشخصي ملوثًا بحساباتك الحقيقية.
- إذا كنت تحتاج فصلًا قويًا بين التطبيقات.
- إذا كان نموذج التهديد يتطلب تحكمًا أعلى.

عندها تنتقل للفصول القادمة: Whonix ثم Qubes.

Persistent Plausible Deniability باستخدام Whonix داخل Tails

هذا جزء متقدم اختياري. الفكرة العامة هي محاولة الجمع بين بيئة Tails المؤقتة وبعض خصائص العزل أو الإنكار المعقول عبر Whonix داخلها. لكنه ليس مناسبًا للمبتدئين، لأن التعقيد يزيد فرصة الخطأ.

1 Advanced Concept

ليس مطلوبًا لفهم الأساسيات. ابدأ بـ Tor Browser وTails العادي قبل أي تركيب متقدم.

2 More Moving Parts

كل طبقة إضافية تعني إعدادات أكثر، أخطاء محتملة أكثر، واختبارات أكثر قبل الاعتماد عليها.

3 Not a Magic Shield

الإنكار المعقول ليس ضمانًا مطلقًا، وقد يفشل حسب الخصم والقانون والسياق والأدلة المحيطة.

إذا لم تكن تفهم Whonix جيدًا، لا تبدأ بهذا الجزء. التعقيد غير المفهوم قد يضر أكثر مما يفيد.

Checklist الفصل السابع

- [ ] **هل اخترت Tor Browser أو Tails بناءً على Threat Model؟**
  لا تختار المسار لأنه "الأقوى"، بل لأنه مناسب لهدفك ومهاراتك ووقتك.
- [ ] **هل حدّثت الأدوات من مصادرها الرسمية؟**
  لا تعتمد على روابط مجهولة أو نسخ معدلة من أطراف غير موثوقة.
- [ ] **هل تجنبت الحسابات الشخصية داخل Tor/Tails؟**
  تسجيل الدخول بحساب حقيقي قد يكسر العزل فورًا.
- [ ] **هل تركت إعدادات Tor Browser افتراضية قدر الإمكان؟**
  التعديلات العشوائية قد تجعل بصمتك أكثر تميزًا.
- [ ] **هل اختبرت Tails USB قبل الاعتماد عليه؟**
  تأكد من الإقلاع، الشبكة، الكيبورد، الوقت، والتوافق مع جهازك.

الخلاصة النهائية للفصل

الفصل السابع يقدم أول تطبيق عملي حقيقي: Tor Browser كبداية سريعة، وTails كبيئة مؤقتة أكثر فصلًا. كلاهما مهم، لكنهما لا يمنعان أخطاء المستخدم مثل خلط الحسابات، نشر معلومات شخصية، تنزيل ملفات خطرة، أو تعديل الإعدادات بلا فهم.

Takeaway: عليك معرفة أن Tor Browser وTails ليسا "هوية مجهولة" بحد ذاتهما؛ هما أدوات داخل منظومة أكبر تشمل العزل، السلوك، الملفات، والجهاز.

Chapter 8 • The Whonix Route

الفصل الثامن: مسار Whonix والعزل عبر الآلات الافتراضية

هذا الفصل ينتقل من Tor Browser وTails إلى عزل أقوى باستخدام Whonix داخل VirtualBox. الفكرة الأساسية هي فصل حركة الشبكة عن بيئة العمل: Whonix Gateway يتعامل مع Tor، وWhonix Workstation تستخدمه للوصول للإنترنت، مما يقلل احتمال تسريب الاتصال الأصلي.

2	3	4	1
VMs أساسية	Host OS Options	Guest VM Choices	قاعدة: العزل قبل الاتصال

فكرة الفصل

Whonix يعتمد على فصل الأدوار. بدل أن يتصل النظام مباشرة بالإنترنت، يتم استخدام **Whonix Gateway** كبوابة Tor، و**Whonix Workstation** كبيئة العمل التي لا تعرف اتصالك الحقيقي مباشرة.

- Gateway يتعامل مع Tor والاتصال الخارجي.
- Workstation هي البيئة التي تعمل داخلها.
- الهدف هو تقليل تسريبات IP من التطبيقات.
- VirtualBox يحتاج إعدادات أمان وانضباط.
- التعقيد أعلى من Tor Browser وTails.

الخلاصة: Whonix ليس مجرد Tor داخل VM؛ هو تصميم عزل بين طبقة الاتصال وطبقة الاستخدام.

Dedicated Laptop

قبل Whonix، يناقش المسار فكرة استخدام لابتوب مخصص للأنشطة الحساسة. السبب أن الجهاز الشخصي يحتوي عادة على حسابات، ملفات، Telemetry، معرفات، وسجل استخدام قد يربطك.

الخطر

تشغيل Whonix على جهازك اليومي قد يترك آثارًا، أو يخلط الحسابات، أو يربط بيئة العزل بجهاز معروف بهويتك.

Personal Device

Identity Link

التخفيف

استخدم جهازًا مخصصًا قدر الإمكان، واضبط BIOS/UEFI، وقلل المكونات غير الضرورية، ولا تخلطه مع استخدامك الشخصي.

Dedicated Device

Isolation

خريطة مسار Whonix

المرحلة	ماذا تفعل؟	الهدف	نقطة الحذر
Dedicated Laptop	استخدام جهاز مخصص إن أمكن	تقليل ربط البيئة بالهوية الشخصية	لا تخلط الحسابات والملفات الشخصية
Host OS	اختيار Linux أو macOS أو Windows كالنظام المثبت	تحديد قاعدة تشغيل VirtualBox والـ VMs	كل Host OS له تسريبات ومخاطر مختلفة

VirtualBox	تثبيت وضبط إعدادات الافتراضية	تشغيل Whonix Gateway وWorkstation	لا تفعّل USB/3D/ميزات غير ضرورية
Connectivity	اختيار Tor فقط أو Tor over VPN أو VPN over Tor	تحديد مسار الشبكة	المسارات المعقدة تزيد احتمال الخطأ
Whonix VMs	استيراد Gateway وWorkstation وتحديثهما	بناء بيئة Tor معزولة	خذ Snapshot بعد التحديث
Guest VM	اختيار Whonix/Linux/Windows/Android/macOS VM	تشغيل التطبيقات المطلوبة خلف Gateway	كل Guest له مخاطر وتسريبات مختلفة

Picking Your Host OS

الـ Host OS هو النظام المثبت على اللابتوب ويشغّل VirtualBox. تقسم الخيارات إلى Linux وmacOS وWindows. اختيار Host OS مهم لأنه الطبقة التي قد ترى الجهاز، الشبكة، ملفات VMs، وبعض آثار الاستخدام.

1 Linux Host OS

خيار قوي ومرن لمن يملك خبرة تقنية. يعطي تحكمًا أكبر، لكنه يحتاج فهمًا للنظام والشبكات والتحديثات والصلاحيات.

2 macOS Host OS

قابل للاستخدام، لكن بعض إعدادات الشبكة والعزل تحتاج خطوات إضافية، خصوصًا عند محاولة منع Host OS من الوصول المباشر للإنترنت.

3 Windows Host OS

سهل للكثيرين، لكنه يحتوي Telemetry وخدمات وخلفيات كثيرة. يحتاج ضبط خصوصية وانتباهًا أكبر لعدم خلط الاستخدام الشخصي بالحساس.

4 Host OS Risk

إذا كان Host OS متصلًا بحساباتك الشخصية أو شبكتك المعتادة، فقد يضعف العزل حتى لو كانت VMs مضبوطة.

مهم: لا تعتبر الـ Host OS محايدًا. هو أساس بيئة Whonix، وأي تسريب منه قد يكسر العزل.

BIOS / UEFI

قبل تشغيل VMs، يجب التفكير في إعدادات Firmware والعتاد، لأن بعض الميزات قد تضيف مخاطر أو توسع سطح الهجوم.

- حدّث Firmware بحذر ومن مصدر رسمي.
- راجع Secure Boot حسب النظام المستخدم.
- عطّل الأجهزة غير المطلوبة إن أمكن.
- استخدم كلمة مرور BIOS/UEFI عند الحاجة.
- قلل boot options غير الضرورية.

لا تجعل الجهاز المخصص نسخة من جهازك الشخصي.

VirtualBox on Host OS

VirtualBox هو الطبقة التي تشغّل Whonix. هناك عدة إعدادات لتقليل المخاطر مثل عدم تفعيل ميزات غير ضرورية، تعطيل USB Controller، عدم تفعيل 3D Acceleration، وأخذ Snapshots بعد التحديث.

Connectivity Method

اختيار طريقة الاتصال يحدد مسار البيانات. قد تستخدم Tor فقط، أو Tor over VPN، أو VPN over Tor، أو طبقات أكثر تعقيدًا. كلما زاد التعقيد زادت الحاجة للفهم والاختبار.

- لا تفعّل 3D Acceleration.
- لا تفعّل Serial Port.
- أزل Floppy وCD/DVD إذا لم تكن مطلوبة.
- لا تفعّل Remote Display Server.
- لا تربط USB devices بالـ VM بلا حاجة.
- خذ Snapshot بعد إعداد VMs وتحديثها.

ميزات الراحة داخل VM قد تكون قنوات تسريب. فعّل فقط ما تحتاجه فعلًا.

Tor Only

أبسط خيار داخل Whonix. مناسب كبداية إذا كان Tor متاحًا.

Tor over VPN

المستخدم → Tor → VPN. يخفي استخدام Tor عن بعض الشبكات، لكنه يضيف ثقة بالـ VPN.

VPN over Tor

المستخدم → VPN → Tor. أكثر تعقيدًا وقد يتطلب إعدادات إضافية داخل VM.

Bridges

تستخدم عند حجب Tor أو مراقبته في بيئة اتصال معادية.

لا تضف VPN فقط لأنه "يزيد الأمان". أحيانًا يزيد التعقيد ويضيف جهة ثقة جديدة.

Whonix Virtual Machines

يتكون Whonix عادة من VMين أساسيين: Gateway وWorkstation. Gateway يتصل بـ Tor، وWorkstation تستخدم Gateway فقط. الهدف أن التطبيقات داخل Workstation لا تصل للشبكة مباشرة، بل تمر عبر Gateway.

المكوّن	الدور	ماذا يجب أن تفعل؟	ماذا تتجنب؟
Whonix Gateway	بوابة Tor والاتصال الخارجي	تحديثه، ضبط الاتصال، استخدام Bridges عند الحاجة	تشغيل أنشطة شخصية داخله
Whonix Workstation	بيئة العمل والتصفح والتطبيقات	استخدامها للأنشطة الحساسة خلف Gateway	ربطها بحساباتك الشخصية أو ملفاتك الحقيقية
Snapshots	نقطة رجوع نظيفة بعد الإعداد	خذ Snapshot بعد التحديث والإعداد الأساسي	الاعتماد على بيئة ملوثة أو غير معروفة الحالة
Updates	تقليل الثغرات والمشاكل	حدّث Gateway وWorkstation بانتظام	تشغيل نسخة قديمة لفترة طويلة

Whonix يعطيك فصلًا هندسيًا بين الاتصال والعمل، لكن السلوك الخاطئ داخل Workstation ما زال خطرًا.

Pick Your Guest Workstation VM

يمكنك استخدام Whonix Workstation الافتراضي، أو إعداد VM مخصص يعمل خلف Whonix Gateway. الاختيار يعتمد على التطبيقات المطلوبة، مستوى المهارة، ومتطلبات العزل.

1 Whonix Workstation

الخيار الموصى به كبداية. مصمم للعمل مع Gateway ويقلل احتمالات التسريب مقارنة بإعدادات مخصصة.

KeePassXC

إدارة كلمات المرور داخل مسار Whonix يجب أن تكون منفصلة ومنظمة. لا تخلط قاعدة بيانات حساباتك الشخصية مع حسابات الهوية الحساسة.

- قاعدة بيانات منفصلة للهويات الحساسة.
- كلمات مرور طويلة وفريدة.
- لا تحفظها في Cloud شخصي.

2 Linux VM

مناسب لمن يحتاج أدوات Linux معينة، لكنه يتطلب ضبط الشبكة خلف Whonix Gateway بعناية.

3 Windows VM

مفيد إذا كنت تحتاج برامج Windows، لكنه يحتوي Telemetry ومخاطر بصمة أعلى ويتطلب ضبط خصوصية.

4 Android / macOS VM

ممكن في بعض الحالات، لكن التعقيد أعلى، والدعم والتسريبات تختلف حسب النظام والتطبيقات.

- احتفظ بنسخ احتياطية مشفرة.
- لا تنسخ كلمات المرور عبر Host OS بلا حاجة.

فصل كلمات المرور جزء من فصل الهوية.

Optional: Cut Off Host OS Internet Access

من الأفكار المتقدمة في المسار محاولة منع الـ Host OS من الوصول المباشر للإنترنت، والسماح فقط للـ VMs بالاتصال. الهدف تقليل احتمالات تسريب من النظام الأساسي، لكن الإعداد أكثر تعقيدًا ويحتاج اختبارًا جيدًا.

الطريقة	الفكرة	الميزة	العيب
Lazy Way	إعداد أبسط يسمح للـ VM بالوصول للشبكة مع اعتماد أكبر على Host	أسهل في التشغيل	قد يعرّض Gateway أو Host لمخاطر أكبر
Route Deletion	حذف Gateway من Host بعد الاتصال بالشبكة	يمنع Host من الإنترنت مؤقتًا	قد يعاد ضبطه عند إعادة الاتصال
Bridge VM	استخدام VM وسيطة مع USB Wi-Fi Dongle بين Host وWhonix	عزل أقوى وأكثر نظافة	أعقد ويتطلب عتادًا إضافيًا وفهمًا للشبكات

هذه الإعدادات متقدمة. لا تعتمد عليها قبل اختبار التسريبات وفهم مسار الشبكة كاملًا.

أخطاء شائعة

- استخدام Host OS شخصي مليء بالحسابات.
- تشغيل Workstation بحسابات حقيقية.
- تفعيل USB أو Shared Clipboard بلا حاجة.
- عدم تحديث Gateway وWorkstation.
- عدم أخذ Snapshot بعد الإعداد النظيف.
- إضافة VPN بدون فهم المسار.

أفضل ممارسات

- استخدم جهازًا مخصصًا إن أمكن.
- ابدأ بـ Whonix Workstation الرسمي.
- حدّث VMs قبل الاستخدام.
- خذ Snapshot بعد الإعداد.
- قلل ميزات التكامل بين Host وVM.
- اختبر IP وDNS والتسريبات بعد الإعداد.

البساطة المضبوطة أفضل من تعقيد غير مفهوم.

أسئلة فحص سريعة

- هل Host OS مرتبط بهويتي؟
- هل Workstation تصل فقط عبر Gateway؟
- هل عطلت USB والميزات غير الضرورية؟
- هل أخذت Snapshot نظيفًا؟
- هل اختبرت Tor connectivity؟
- هل فصلت كلمات المرور والحسابات؟

إذا لم تفهم مسار الشبكة، لا تعتبر الإعداد آمنًا.

✅ Checklist الفصل الثامن

- ✓ **هل الجهاز أو Host OS منفصل قدر الإمكان؟**
  لا تبني بيئة Whonix الحساسة فوق جهاز مليء بحساباتك الشخصية دون فهم المخاطر.

- ✓ **هل ضبطت VirtualBox بدون ميزات غير ضرورية؟**
  تجنب shared features، 3D acceleration، USB، وRemote Display إلا عند الحاجة المبررة.

- ✓ **هل استوردت وحدثت Whonix Gateway وWorkstation؟**
  استخدم المصادر الرسمية، حدّث النظامين، ثم خذ Snapshot نظيفًا.

- ✓ **هل اخترت Guest VM مناسبًا؟**
  ابدأ بـ Whonix Workstation، ولا تنتقل لـ Windows/Android/macOS VM إلا إذا احتجت وفهمت المخاطر.

- ✓ **هل اختبرت التسريبات بعد الإعداد؟**
  افحص IP وDNS وTor connectivity قبل استخدام البيئة لأي نشاط حساس.

📝 الخلاصة النهائية للفصل

الفصل الثامن يقدم مسارًا أقوى من Tor Browser وTails عبر Whonix، لكنه أعقد ويحتاج انضباطًا أعلى. قوة Whonix تأتي من الفصل بين Gateway وWorkstation، لكن هذا العزل يضعف إذا كان Host OS ملوثًا، أو كانت إعدادات VirtualBox مفتوحة، أو تم خلط الحسابات والملفات والهويات داخل نفس البيئة.

Takeaway: نظام Whonix يعطيك عزلًا معماريًا جيدًا، لكن نجاحه يعتمد على ضبط Host OS وVirtualBox وVMs، ثم اختبار التسريبات قبل الاستخدام.

Chapter 9 • The Qubes Route

الفصل التاسع: مسار Qubes OS والعزل بالتقسيم

هذا الفصل يقدم Qubes OS كمسار متقدم يعتمد على virtualization وcompartmentalization. بدل تشغيل كل شيء داخل نظام واحد، يتم فصل الأنشطة داخل Qubes مختلفة. هذا يقلل أثر الاختراق أو الخطأ، ويجعل كل مهمة داخل حجرة مستقلة حسب درجة الثقة والهدف.

4	3	2	1
طبقات عزل	VM Types مهمة	مسارات شبكة	قاعدة: افصل كل مهمة

فكرة الفصل

Qubes OS ليس توزيعة Linux عادية. هو نظام مبني حول فكرة أن كل تطبيق أو مهمة يجب أن تعمل داخل بيئة معزولة. لذلك يمكن فصل العمل، التصفح، الملفات غير الموثوقة، الحسابات الحساسة، وWhonix داخل Qubes مختلفة.

- يعتمد على Xen virtualization.
- يفصل التطبيقات والمهام داخل Qubes مستقلة.
- يدمج Whonix افتراضيًا لسيناريوهات Tor.
- مناسب للمستخدمين التقنيين أكثر من المبتدئين.
- قوته في الفصل بين الثقة، وليس فقط إخفاء الشبكة.

الخلاصة: Qubes يحاول تقليل الضرر عند حدوث خطأ؛ لأن الخطأ يبقى داخل Qube محددة بدل النظام كاملًا.

Compartmentalization

المبدأ الأساسي هو تقسيم الاستخدامات حسب مستوى الثقة. مثلًا: Qube للعمل، Qube للتصفح، Qube للملفات غير الموثوقة، Qube للحسابات الحساسة، وQube يستخدم Whonix للوصول عبر Tor.

الفائدة

إذا تم اختراق تطبيق داخل Qube منخفضة الثقة، لا يعني ذلك بالضرورة وصول المهاجم لباقي الملفات والحسابات في Qubes الأخرى.

Isolation

Damage Control

الحدود

Qubes لا يمنع الأخطاء البشرية مثل نسخ بيانات بين Qubes خطأ، تسجيل الدخول بحساب حقيقي، أو مشاركة ملف يكشف الهوية.

User Mistakes

Operational Risk

خريطة Qubes OS

المكوّن	الدور	مثال استخدام	نقطة الحذر
dom0	النظام الإداري المركزي	إدارة النوافذ، إعدادات Qubes، التحكم العام	لا تستخدمه للتصفح أو فتح الملفات
AppVM	بيئة تشغيل التطبيقات اليومية	تصفح، بريد، كتابة، عمل	افصل AppVM حسب مستوى الثقة
TemplateVM	مصدر النظام والتطبيقات للـ AppVMs	Debian Template أو Fedora Template	التحديث يتم غالبًا في Template وليس AppVM
DisposableVM	بيئة مؤقتة تُحذف بعد الاستخدام	فتح ملف مشبوه أو رابط غير موثوق	لا تحفظ فيها بيانات تريد الاحتفاظ بها
sys-net / sys-firewall	إدارة الشبكة والجدار الناري	فصل كرت الشبكة عن باقي النظام	أي خطأ في الشبكة يؤثر على الاتصال
Whonix Qubes	توجيه الاتصال عبر Tor	anon-whonix وsys-whonix	لا تخلط هوية Tor مع هوية شخصية

Installation & Hardware Requirements

Qubes OS يحتاج توافقًا جيدًا مع العتاد وموارد أعلى من الأنظمة العادية. السبب أن كل مهمة تعمل داخل VM، وكل VM تحتاج RAM وCPU ومساحة. التجربة المريحة تحتاج RAM أعلى، وأن أقل من 8GB غير مناسب غالبًا، بينما 16GB أو أكثر أفضل للاستخدام العملي.

1 Hardware Compatibility

قبل التثبيت، تحقق من توافق اللابتوب مع Qubes، خصوصًا GPU، Wi-Fi، virtualization، وsleep/wake.

2 RAM Requirement

لأن كل Qube تعمل كـ VM، الذاكرة مهمة جدًا. كلما زادت Qubes المفتوحة زاد استهلاك RAM.

3 Installation Discipline

استخدم ISO من المصدر الرسمي، تحقق من سلامة التنزيل، وجهّز خطة قبل التثبيت.

4 Not Beginner-Friendly

Qubes قوي، لكنه ليس المسار الأسهل. يحتاج فهمًا لـ VMs والشبكات والتحديثات وفصل المهام.

مهم: لا تبدأ Qubes إذا كنت لا تستطيع إدارة VMs وتحديثات وقواعد عزل متعددة.

Lid Closure Behavior

سلوك إغلاق غطاء اللابتوب مهم في الأجهزة المحمولة. إذا دخل الجهاز Sleep بطريقة غير متوقعة، قد تتعطل الشبكة أو تتوقف Qubes أو يحدث سلوك غير مناسب أثناء نشاط حساس.

- اختبر sleep/wake قبل الاستخدام.
- لا تعتمد على الإغلاق السريع كإجراء أمني.
- اضبط سلوك الغطاء حسب الحاجة.
- تأكد أن الشبكة تعود كما تتوقع.
- لا تترك جلسات حساسة مفتوحة.

السلوك الفيزيائي للجهاز جزء من OPSEC.

Connectivity Method

في Qubes، الشبكة ليست مجرد إعداد واحد. يمكن بناء مسارات مثل sys-net → sys-firewall → AppVM، أو استخدام sys-whonix لتوجيه الاتصال عبر Tor، أو إعداد VPN ProxyVM عند الحاجة.

Normal Route

AppVM → sys-firewall → sys-net. مناسب للاستخدام العادي غير المجهول.

Tor Route

anon-whonix → sys-whonix. مناسب لأنشطة Tor داخل Qubes.

VPN ProxyVM

إضافة VM كوسيط VPN لتوجيه بعض Qubes عبر VPN.

Offline Qube

Qube بدون شبكة للملفات الحساسة أو العمل المحلي.

Updating Qubes OS

ضرورة إبقاء Qubes OS محدثًا قبل أي نشاط حساس، خصوصًا Browser VMs. التحديثات قد تأخذ وقتًا إذا كانت تمر عبر Tor، لذلك يجب التخطيط لها قبل وقت الاستخدام.

- حدّث Qubes قبل الأنشطة الحساسة.
- حدّث Templates مثل Debian/Fedora.
- حدّث Whonix templates عند الحاجة.
- لا تستخدم Browser VM قديمة.
- خطط لوقت التحديث إذا كان عبر Tor.

بيئة معزولة لكنها قديمة ليست آمنة بما يكفي.

لا تخلط Qube شخصية مع sys-whonix أو VPN ProxyVM دون فهم واضح للمسار.

Hardening Qubes OS

Qubes يعزل التطبيقات افتراضيًا، لكن يمكن تحسين الأمان بإجراءات إضافية، مثل استخدام AppArmor في Debian/Whonix أو SELinux في Fedora، وضبط الصلاحيات، وتقليل الميزات غير الضرورية.

الإجراء	أين يستخدم؟	الهدف	ملاحظة
AppArmor	Debian / Whonix templates	تقييد صلاحيات التطبيقات	مفيد لكنه يحتاج فهمًا للقواعد
SELinux	Fedora templates	Mandatory Access Control	مناسب أكثر لعالم Fedora
Minimal Templates	Templates مخصصة	تقليل سطح الهجوم	تحتاج مهارة أعلى
DisposableVMs	فتح ملفات وروابط غير موثوقة	تقليل بقاء الآثار والاختراقات	لا تحفظ بيانات مهمة بداخلها
Firewall Rules	AppVMs وProxyVMs	تقييد الاتصال حسب الحاجة	كل Qube يجب أن تملك قواعدها المناسبة

مهم: Hardening المتقدم قد يكسر وظائف أو يزيد التعقيد. لا تطبقه عشوائيًا.

Setup the VPN ProxyVM

VPN ProxyVM يسمح بتوجيه Qubes معينة عبر VPN. هذا مفيد إذا كان نموذج التهديد يحتاج VPN، لكنه ليس مطلوبًا دائمًا. إذا كان Tor كافيًا، أو VPN غير مناسب، يمكن تخطي هذا الجزء.

1 Decide First

لا تضف VPN فقط لأنه يبدو "أقوى". حدد لماذا تحتاجه وما الجهة التي تثق بها.

2 Create ProxyVM

خصص Qube تعمل كوسيط VPN بدل تثبيت VPN داخل كل AppVM عشوائيًا.

3 Route Specific Qubes

اربط فقط الـ Qubes التي تحتاج VPN بهذا المسار، واترك البقية حسب نموذج الاستخدام.

4 Test Leaks

افحص IP وDNS وتسريبات WebRTC بعد إعداد VPN ProxyVM وقبل استخدامه.

VPN داخل Qubes بدون فهم routing قد يعطيك إحساسًا كاذبًا بالأمان.

Safe Browser Qube

يمكن إعداد Qube مخصصة للتصفح الآمن، منفصلة عن البريد والعمل والملفات الشخصية. الهدف أن المتصفح لا يكون داخل نفس بيئة الحسابات أو الملفات الحساسة.

- Qube مستقلة للتصفح العام.
- Qube أخرى للحسابات الحساسة.
- Qube عبر Whonix للأنشطة المجهولة.
- DisposableVM للروابط غير الموثوقة.
- لا تخلط الجلسات داخل نفس Qube.

افصل المتصفح حسب الثقة والهوية.

Setup an Android VM

يذكر إعداد Android VM كخيار ضمن Qubes. هذا قد يكون مفيدًا عند الحاجة لتطبيقات Android، لكنه يضيف تعقيدًا ومخاطر إضافية لأن تطبيقات الهاتف غالبًا تعتمد على معرفات، حسابات، إشعارات، وصلاحيات كثيرة.

- استخدمه فقط عند الحاجة الفعلية.
- لا تربطه بحساب Google الشخصي.
- راجع صلاحيات التطبيقات.
- افصله عن Qubes الحساسة.
- اختبر الشبكة والتسريبات.

Android داخل VM لا يلغي مخاطر تطبيقات الهاتف وسلوكها.

KeePassXC in Qubes

KeePassXC داخل Qubes يجب أن يستخدم بفلسفة الفصل. يمكنك تخصيص Qube آمنة لإدارة كلمات المرور، وعدم فتح قاعدة البيانات داخل Qubes منخفضة الثقة.

Password Vault Qube

Qube مخصصة لإدارة كلمات المرور فقط.

Separate Databases

قاعدة شخصية، قاعدة عمل، وقاعدة هويات حساسة.

No Random Copying

لا تنسخ كلمات المرور بين Qubes بلا حاجة.

Encrypted Backup

احتفظ بنسخة احتياطية مشفرة ومفصولة.

تصميم Qubes عملي مقترح

Qube	الاستخدام	الشبكة	مستوى الثقة
personal	حسابات شخصية عادية	sys-firewall	متوسط
work	عمل أو دراسة	sys-firewall أو VPN ProxyVM	متوسط إلى عالي
vault	كلمات مرور وملفات حساسة	None / Offline	عالي
untrusted	ملفات وروابط غير موثوقة	sys-firewall أو Disposable	منخفض
anon-whonix	نشاط مجهول عبر Tor	sys-whonix	حساس
disposable	فتح مرفقات وروابط مؤقتة	حسب الحاجة	منخفض ومؤقت

أخطاء شائعة

- استخدام Qube واحدة لكل شيء.
- فتح ملفات غير موثوقة داخل Qube حساسة.
- نسيان تحديث Templates.
- خلط anon-whonix مع حسابات شخصية.
- نسخ ملفات وكلمات مرور بين Qubes بلا

أفضل ممارسات

- افصل Qubes حسب المهمة والثقة.
- استخدم DisposableVM للملفات المشبوهة.
- اجعل vault بدون شبكة.
- حدّث Templates بانتظام.
- استخدم Whonix Qubes للأنشطة

أسئلة فحص سريعة

- هل هذه المهمة تحتاج Qube مستقلة؟
- هل هذه Qube تحتاج إنترنت أصلًا؟
- هل الملف موثوق أم يجب فتحه Disposable؟
- هل Template محدثة؟
- هل هذه Qube تستخدم sys-whonix أو

وعي.

- إضافة VPN دون اختبار التسريبات.

المجهولة.

- اختبر routing بعد كل تغيير.

قوة Qubes في الفصل، وليس في كثرة الأدوات.

sys-firewall؟

- هل نسخت بيانات بين Qubes بلا حاجة؟

إذا لم تعرف مسار الشبكة، لا تعتبر العزل صحيحًا.

✅ Checklist الفصل التاسع

✓ **هل جهازك مناسب لـ Qubes OS؟**

تحقق من RAM، virtualization، Wi-Fi، GPU، والتوافق قبل الاعتماد عليه.

✓ **هل فصلت Qubes حسب مستوى الثقة؟**

personal، work، vault، untrusted، anon-whonix، disposable.

✓ **هل جعلت الملفات غير الموثوقة داخل DisposableVM؟**

لا تفتح المرفقات المشبوهة داخل Qube تحتوي ملفات أو حسابات مهمة.

✓ **هل حدّثت Qubes وTemplates قبل الاستخدام؟**

خصوصًا Browser VMs وWhonix/Fedora/Debian templates.

✓ **هل اختبرت الشبكة بعد إعداد VPN ProxyVM أو sys-whonix؟**

افحص IP وDNS وTor قبل أي نشاط حساس.

📝 الخلاصة النهائية للفصل

الفصل التاسع يقدم Qubes OS كأقوى مسار عزل في هذا الجزء من المقرر. قوته ليست في إخفاء IP فقط، بل في تقسيم النظام إلى Qubes حسب الثقة والاستخدام. لكنه يتطلب عتادًا مناسبًا، فهمًا جيدًا للـ virtualization، تحديثات مستمرة، وانضباطًا في نقل الملفات والحسابات بين Qubes.

Takeaway: نظام Qubes OS لا يجعلك مجهولًا تلقائيًا؛ هو يمنحك بيئة عزل قوية، والنجاح يعتمد على تصميم Qubes صحيح، فصل الهويات، واختبار مسارات الشبكة.

الحزمة العملية الثالثة: Tor, Tails, Whonix و Qubes OS

هذه الصفحة تجمع الجانب العملي من الفصول 7 إلى 9. الهدف هو تحويل مسارات Tor Browser، Tails، Whonix، وQubes OS إلى خطوات تشغيل وفحص واضحة: اختيار المسار، اختبار التسريبات، ضبط العزل، إدارة الـ VMs، استخدام Snapshots، وفصل المهام حسب مستوى الثقة.

4	8	5	1
مسارات عملية	اختبارات عزل	Checklists	Workflow نهائي

هدف هذه الصفحة

الفصول 7–9 تنقل المقرر من المفاهيم والتجهيزات إلى بيئات تشغيل حقيقية. هذه الصفحة تساعدك تختار المسار المناسب، ثم تفحصه عمليًا قبل استخدامه لأي نشاط حساس.

Tor Browser

حل سريع للتصفح عبر Tor. مناسب كبداية، لكنه لا يعزل النظام بالكامل.

Simple Route

Tails

نظام Live من USB لتقليل الأثار المحلية والعمل في جلسة مؤقتة.

Live USB

Whonix

عزل شبكي عبر Gateway وWorkstation داخل VirtualBox.

VM Isolation

Qubes OS

تقسيم المهام داخل Qubes مختلفة حسب الثقة والاستخدام.

Compartmentalization

Tor Browser Setup Checklist

Tor Browser مناسب كبداية، لكن يجب تشغيله بطريقة لا تجعل بصمتك مميزة ولا ترتبك بحسابات الحقيقية.

- **حمّل Tor Browser من المصدر الرسمي**
  تجنب النسخ المعدلة أو الروابط العشوائية.
- **اترك الإعدادات الافتراضية قدر الإمكان**
  الإضافات والتعديلات الكثيرة قد تجعل بصمتك فريدة.
- **لا تدخل بحساباتك الشخصية**
  تسجيل الدخول يكسر الفصل بين هويتك والجلسة.

Tor Browser Official Download
استخدم الموقع الرسمي فقط لتنزيل Tor Browser.

Tails USB Prep

Tails يحتاج USB وإقلاع صحيح. لا تنتظر وقت الحاجة الفعلية لتكتشف أن الجهاز لا يقلع أو أن الشبكة لا تعمل.

- **استخدم USB موثوقًا**
  يفضل 32GB أو أكثر، ومن مصدر معلوم.
- **اختبر الإقلاع مسبقًا**
  تأكد من BIOS/UEFI، الكيبورد، الشبكة، والوقت.
- **لا تخلط ملفاتك الشخصية داخل الجلسة**
  Tails مفيد فقط إذا حافظت على فصل الهوية والملفات.

Tails Official Installation Guide
اتبع دليل التثبيت الرسمي حسب نظامك.

Leak Testing Before Use

قبل الاعتماد على أي مسار، افحص التسريبات الأساسية. الاختبار لا يعني أنك مجهول بالكامل، لكنه يكشف الأخطاء الواضحة في IP وDNS وTor WebRTC routing.

الاختبار	الرابط	متى تستخدمه؟	ماذا تبحث عنه؟
Tor Check	check.torproject.org	بعد تشغيل Tor/Tails/Whonix	هل الاتصال يمر عبر Tor؟
DNS Leak	dnsleaktest.com	بعد VPN أو ProxyVM أو Whonix	هل DNS يخرج من جهة غير متوقعة؟
Browser Leaks	browserleaks.com	بعد إعداد المتصفح	WebRTC، Canvas، Fonts، WebGL، Timezone
Cover Your Tracks	coveryourtracks.eff.org	عند فحص بصمة المتصفح	هل المتصفح فريد جدًا؟
IP Check	whatismyip.com	قبل وبعد تشغيل المسار	هل IP الحقيقي ظاهر؟
Qubes Routing Test	داخل كل Qube	بعد تغيير NetVM أو ProxyVM	هل هذه Qube تخرج عبر المسار الصحيح؟

قاعدة: لا تستخدم البيئة قبل اختبارها. أي تغيير في الشبكة أو VM يستدعي إعادة فحص التسريبات.

Whonix Practical Setup

Whonix يعتمد على جهازين افتراضيين أساسيين: Gateway وWorkstation. الهدف أن التطبيقات داخل Workstation لا تخرج مباشرة للإنترنت، بل تمر عبر Gateway.

الإجراء	الهدف
استيراد Gateway وWorkstation من المصدر الرسمي	ضمان أن البيئة أصلية وغير معدلة
تحديث كلا الـ VMs	تقليل الثغرات قبل الاستخدام
إيقاف USB 3D Shared Features غير الضرورية	تقليل فتوات التسريب بين VM وHost
أخذ Snapshot بعد الإعداد النظيف	توفير نقطة رجوع آمنة
فحص Tor/IP/DNS من Workstation	التأكد من أن المسار صحيح

لا تستخدم Workstation كهوية شخصية. أي حساب أو ملف حقيقي داخلها قد يربط الهوية.

Qubes Practical Layout

قوة Qubes في الفصل بين المهام. لا تجعل Qube واحدة لكل شيء. صمم Qubes حسب الثقة: شخصية، عمل، مجهولة، غير موثوقة، وقلو بدون شبكة.

Qube	الاستخدام	الشبكة
vault	كلمات مرور ومفاتيح حساسة	None
personal	حسابات شخصية	sys-firewall
work	عمل أو دراسة	sys-firewall أو VPN ProxyVM
untrusted	روابط وملفات غير موثوقة	DisposableVM
anon-whonix	أنشطة Tor	sys-whonix

كل مهمة لها Qube. كل Qube لها مستوى ثقة. كل مستوى ثقة له مسار شبكة مناسب.

Route Selection Matrix

الحالة	المسار المناسب	لماذا؟
تصفح سريع وتهديد منخفض	Tor Browser	سهل وسريع
جلسة مؤقتة من USB	Tails	يقلل الأثار المحلية
تطبيقات داخل VM تحت Tor	Whonix	يفصل Gateway عن Workstation
عدة هويات ومهام مختلفة	Qubes OS	يعزل كل مهمة داخل Qube
فتح ملف غير موثوق	Qubes DisposableVM	يقلل أثر الملف الخبيث
بيانات حساسة لا تحتاج إنترنت	Qubes vault أو جهاز Offline	يمنع تسريب الشبكة

VirtualBox Hardening

- عطّل 3D Acceleration.
- عطّل USB Controller إلا إن لم تحتاجه.
- لا تستخدم Shared Clipboard إلا عند الحاجة.
- لا تستخدم Shared Folders مع ملفات حساسة.
- عطّل Remote Display.
- خذ Snapshot بعد الإعداد النظيف.

ميزات الراحة قد تصنع قنوات تسريب.

Snapshot Strategy

- Snapshot بعد التثبيت.
- Snapshot بعد التحديث.
- Snapshot قبل تجربة إعداد خطير.
- لا تخزن أسرارًا داخل Snapshot مشبوه.
- احذف Snapshots الملوثة.
- وثّق اسم كل Snapshot وسببها.

Snapshot تظيف يوفر نقطة رجوع قبل أن تتراكم الأخطاء.

Password Vault

- استخدم KeePassXC.
- قاعدة منفصلة للهويات الحساسة.
- لا تضع قاعدة كلمات المرور في Qube متصلة بالشبكة.
- احفظ نسخة احتياطية مشفرة.
- لا تسمح كلمات المرور بين Qubes بلا حاجة.
- اجعل vault بدون إنترنت عند الإمكان.

مدير كلمات المرور نفسه يحتاج عزلًا.

Practical Workflow: From Setup to Use

المرحلة	الإجراء	الهدف	فحص قبل الانتقال
اختيار المسار	Tor / Tails / Whonix / Qubes حسب الحاجة	تجنب التعقيد غير الضروري	هل يناسب Threat Model؟
التثبيت	تحميل من المصدر الرسمي والتحقق قدر الإمكان	منع النسخ المعدلة	هل المصدر رسمي؟
التحديث	تحديث النظام أو الـ VMs أو Templates	تقليل الثغرات	هل البيئة محدثة؟
العزل	فصل الحسابات والملفات والـ VMs/Qubes	منع ربط الهويات	هل يوجد خلط بين الهوية الحقيقية والمجهولة؟
اختبار التسريبات	IP / DNS / WebRTC / Tor Check	كشف الأخطاء الواضحة	هل المسار يظهر كما توقعت؟
الاستخدام	استخدام منضبط بدون حسابات شخصية أو ملفات أصلية	الحفاظ على العزل	هل السلوك يتسق؟
الإغلاق	حذف الملفات المؤقتة أو الرجوع إلى Snapshot نظيف	تقليل الأثار	هل بقيت ملفات أو سجلات غير مقصودة؟

Common Failure Modes

- استخدام نفس الحساب الشخصي داخل Tor أو Whonix.
- فتح ملفات مجهولة داخل Qube أو VM حساسة.
- إضافة VPN دون فهم مسار الشبكة.
- تفعيل Shared Clipboard أو USB بلا حاجة.
- عدم تحديث Templates أو الـ VMs.
- عدم اختبار الـ DNS بعد تغيير الإعدادات.
- استخدام Qube واحدة لكل المهام في Qubes OS.
- الاعتماد على الأداة بدل الانضباط التشغيلي.

High-Value Practices

- ابدأ بالمسار الأبسط الذي يلبي حاجتك.
- استخدم المصادر الرسمية فقط.
- اختبر الإعداد قبل الحاجة الفعلية.
- افصل كلمات المرور والحسابات والملفات.
- حدّث Snapshots نظيفة في Whonix.
- استخدم DisposableVM في Qubes للملفات غير الموثوقة.
- اجعل vault بدون شبكة عند الإمكان.
- أعد اختبار التسريبات بعد أي تعديل.

الممارسة الجيدة: كل تعديل في الشبكة أو الهوية يتبعه اختبار تسريب.

Final Checklist: Chapters 7–9

- **هل اخترت المسار بناءً على Threat Model؟**
  Tor Browser للبداية، Tails للجلسات المؤقتة، Whonix لعزل Tor داخل VMs، Qubes للفصل المتقدم.
- **هل حمّلت الأدوات من مصادرها الرسمية؟**
  لا تعتمد على نسخ معدلة أو روابط غير موثوقة.
- **هل حدّثت البيئة قبل الاستخدام؟**
  Tor/Tails/Whonix/Qubes/Templates يجب أن تكون محدثة قدر الإمكان.
- **هل اختبرت IP وDNS وTor routing؟**
  لا تبدأ قبل التأكد من أن المسار يخرج كما تتوقع.
- **هل فصلت الحسابات والملفات وكلمات المرور؟**
  الأداة لا تنقذك إذا خلطت الهوية الحقيقية بالمجهولة.
- **هل لديك خطة رجوع نظيفة؟**
  Snapshot في Whonix، DisposableVM في Qubes، أو جلسة Tails جديدة.

الخلاصة العملية: Tor وTails وWhonix وQubes ليست بدائل عن OPSEC؛ هي تطبيق تساعدك فقط إذا صممت العزل واخترت التسريبات وحافظت على فصل الهوية.

الفصل العاشر: إنشاء الهويات المجهولة على الإنترنت

هذا الفصل ينتقل من إعداد البيئة إلى إنشاء الهوية نفسها. المنصات لا تعتمد فقط على اسم المستخدم وكلمة المرور، بل تستخدم Captchas، رقم الهاتف، البريد، عنوان IP، بصمة المتصفح، السلوك، المعاملات المالية، والمراجعات اليدوية لتقييم الحساب وربطه أو رفضه.

11	3	2	1
طرق تحقق وربط	طبقات هوية	نقاط كسر خطيرة	قاعدة: لا تربط الهويات

فكرة الفصل

إنشاء هوية مجهولة لا يعني فقط اختيار اسم مستعار. المنصة تحاول معرفة: هل أنت إنسان؟ هل بياناتك منطقية؟ هل عنوان IP مريب؟ هل البريد مؤقت؟ هل الهاتف حقيقي؟ هل السلوك يشبه حسابًا آليًا أو حسابًا مكررًا؟

- التحقق من الهاتف قد يكون أقوى رابط بالهوية الحقيقية.
- البريد المؤقت غالبًا يتم رفضه أو وضعه تحت الاشتباه.
- عنوان IP من Tor أو VPN قد يرفع مستوى التدقيق.
- بصمة المتصفح والجهاز قد تربط جلسات مختلفة.
- السلوك واللغة والتفاعل قد يكشفون الهوية مع الوقت.

الخلاصة: الهوية المجهولة تُبنى كمنظومة كاملة: بيئة، بريد، رقم، اسم، سلوك، شبكة، وتاريخ استخدام منفصل.

Captchas

Captchas تستخدم للتمييز بين الإنسان والبوت، لكنها أيضًا قد تكون جزءًا من تقييم المخاطر. الحساب القادم من IP مريب أو بصمة غريبة قد يواجه اختبارات أكثر أو يتم حظره قبل التسجيل.

الخطر

كثرة Captchas أو فشلها قد تعني أن المنصة ترى الاتصال أو البصمة أو السلوك كشيء عالي الخطورة.

Risk Scoring

Bot Detection

التعامل الصحيح

استخدم بيئة نظيفة ومتسقة، لا تغير إعدادات المتصفح بشكل غريب، ولا تكرر محاولات التسجيل بسرعة.

Consistency

Clean Session

خريطة طرق منع المجهولية والتحقق من الهوية

الطريقة	ماذا تفحص؟	الخطر على المجهولية	التعامل العملي
Captchas	هل أنت إنسان أم بوت؟	ترفع التدقيق عند IP أو بصمة مشبوهة	جلسة نظيفة وسلوك طبيعي وغير متكرر
Phone Verification	رقم الهاتف وبلده وقابليته للتتبع	قد يربط الحساب بهويتك مباشرة	رقم منفصل وقانوني وغير مرتبط بحساباتك
E-Mail Verification	نوع البريد وسمعة مزوده	البريد المؤقت أو المعروف قد يرفض أو يرفع الاشتباه	بريد منفصل طويل المدى مع aliases عند الحاجة
User Details Checking	اتساق الاسم، البلد، العمر، اللغة، الصورة	التفاصيل غير المنطقية تكشف أو تعطل الحساب	هوية متسقة لا تستند لتفاصيلك الحقيقية
Proof of ID	وثائق رسمية أو صور هوية	يكسر المجهولية غالبًا	تجنب المنصات التي تتطلب وثائق إذا كان هدفك المجهولية
IP Filters	سمعة IP والبلد وVPN/Tor	قد يرفض التسجيل أو يربط الموقع	اختيار مسار اتصال مناسب وثابت حسب الهوية

		بسلوكك	
Browser Fingerprinting	المتصفح، الخطوط، WebGL، Canvas، الوقت	ربط الجلسات حتى بدون حساب مباشر	بيئة موحدة وعدم إضافة تعديلات غريبة
Behavioral Analysis	التوقيت، السرعة، النمط، التفاعل	السلوك نفسه قد يكشف الحسابات أو يرفع الاشتباه	استخدام طبيعي ومتسق وغير آلي
Financial Transactions	وسيلة الدفع، الاسم، العنوان، KYC	ربط مالي مباشر بالهوية	تجنب الدفع المرتبط بالهوية للحسابات الحساسة
Sign-in with Platform	ربط Google/Apple/Facebook وغيرها	يكسر الفصل بين الحسابات	لا تستخدم تسجيل الدخول عبر حسابات شخصية
Manual Reviews	مراجعة بشرية للبيانات والسلوك	تجميع القرائن الصغيرة يدويًا	اتساق الهوية وتقليل المؤشرات المتناقضة

Phone & E-Mail Verification

التحقق برقم الهاتف والبريد من أكثر نقاط الضعف في إنشاء الهويات. التحقق بالهاتف لا يستخدم فقط للتأكد أنك إنسان، بل قد يساعد المنصة على نزع المجهولية عند الحاجة. كما أن البريد المؤقت أو المفتوح قد يتم رفضه مثل البروكسيات المفتوحة.

1 Phone Number

رقم الهاتف قد يرتبط بشريحة SIM، بلد، مزود خدمة، سجل شراء، أو وثائق تسجيل حسب النظام المحلي.

2 E-Mail Provider Reputation

بعض المنصات ترفض disposable e-mails أو تطلب رقم هاتف لإنشاء بريد جديد، مما يعيدك لنفس المشكلة.

3 E-Mail Aliasing

خدمات aliasing تساعد في عدم كشف البريد الأساسي لكل منصة، لكنها لا تعني مجهولية كاملة.

4 Hard Breakpoint

إذا طلبت المنصة رقمك الحقيقي أو وثائق رسمية، فهذه نقطة كسر قوية للمجهولية.

لا تستخدم رقمك الشخصي أو بريدك الحقيقي لهوية تريد فصلها عنك.

Proof of ID

طلب إثبات الهوية مثل جواز أو بطاقة وطنية أو رخصة غالبًا ينهي فكرة المجهولية على تلك المنصة. تزوير الوثائق ليس مسارًا مقبولًا، وقد يكون غير قانوني في أغلب الأماكن.

- لا تقدم وثائقك الحقيقية لهوية مجهولة.
- لا تستخدم وثائق مزيفة أو معدلة.
- تجنب المنصات التي تتطلب KYC إذا كان هدفك المجهولية.
- افصل بين الحسابات المالية والحسابات المجهولة.
- افهم أن بعض المنصات لا تصلح لهذا الهدف.

بعض المتطلبات لا يمكن تجاوزها بأمان؛ اختر منصة أخرى بدل كسر القانون أو كشف الهوية.

Fingerprinting & IP Filters

حتى لو كان البريد والرقم منفصلين، قد تكشفك الشبكة والبصمة. المنصات قد تنظر إلى عنوان IP، الدولة، سمعة VPN/Tor، WebRTC، Canvas، WebGL، الخطوط، المنطقة الزمنية، واللغة.

IP Reputation

IP من Tor أو VPN معروف قد يسبب Captcha أو رفض أو مراجعة.

Location Mismatch

بلد IP لا يطابق اللغة أو بيانات الحساب قد يثير الشك.

Browser Fingerprint

إعدادات المتصفح قد تربط جلسات أو تميزك عن بقية المستخدمين.

Device Fingerprint

نفس الجهاز أو VM أو المتصفح قد يربط عدة هويات.

الاتساق مهم: البلد، اللغة، التوقيت، البريد، والـ IP يجب ألا يتناقضوا بشكل واضح.

Behavioral & Human Checks

المنصات لا تفحص البيانات التقنية فقط. قد تنظر إلى طريقة التفاعل، سرعة التسجيل، عدد المحاولات، طبيعة الرسائل، علاقات الحساب، وجوده في جهات اتصال الآخرين، ومدى "طبيعية" السلوك.

- لا تنشئ حسابات كثيرة بسرعة.
- لا تستخدم نفس النصوص أو النمط في كل منصة.
- لا تقفل كل إعدادات الخصوصية بطريقة مفاجئة وغريبة فور التسجيل.
- لا تبدأ بنشاط عالي جدًا من حساب جديد.
- اجعل الهوية متسقة منطقيًا مع البلد واللغة والاهتمامات.
- لا تربط الحساب الجديد بحسابات أو جهات اتصالك الحقيقية.

الهوية المجهولة تحتاج سلوكًا طبيعيًا ومنفصلًا، لا مجرد بيانات تسجيل مختلفة.

Financial Transactions, Platform Sign-In & Biometrics

المعاملات المالية، تسجيل الدخول عبر منصة أخرى، والقياسات الحيوية من أقوى طرق الربط. أي دفع ببطاقة شخصية، أو تسجيل دخول عبر Google/Apple/Facebook، أو رفع صورة وجه يمكن أن يكسر العزل بين الهوية المجهولة والحقيقية.

العنصر	لماذا خطير؟	مثال	التعامل الصحيح
Financial Transactions	الدفع غالبًا مرتبط باسم، بطاقة، بنك، عنوان، أو KYC	شراء خدمة للحساب المجهول ببطاقتك الشخصية	تجنب الدفع المرتبط بهويتك عند بناء حساب حساس
Sign-in with Platform	يربط الحساب الجديد مباشرة بحساب موجود	Continue with Google أو Apple ID	أنشئ تسجيلًا مستقلًا ببريد منفصل
Face Recognition	الصورة أو الفيديو قد يربطانك بحسابات وصور سابقة	رفع صورة شخصية لحساب مجهول	تجنب الصور البيومترية للحسابات المجهولة
Live Biometrics	التحقق الحي قد يطلب حركة وجه أو فيديو	منصة تطلب selfie verification	اعتبرها نقطة كسر للمجهولية
Manual Review	مراجع بشري قد يجمع التناقضات الصغيرة	اسم، بلد، IP، لغة، صورة لا تتوافق	هوية متسقة أو تجنب المنصة

Getting Online & Creating New Identities

عند البدء فعليًا، لا تنشئ الهوية من داخل بيئة مرتبطة بك. يجب أن تكون الشبكة، المتصفح، البريد، الرقم، الاسم، السلوك، والملفات كلها منفصلة. الهوية الجديدة يجب أن تكون "نظيفة" ولا تحمل آثارًا من هويتك الأصلية.

الطبقة	ماذا تفصل؟	خطأ يكسر العزل
Network	IP، DNS، Tor/VPN route	التسجيل من شبكة البيت أو IP مرتبط بك
Device / Browser	VM/Qube، بصمة المتصفح، الكوكيز	استخدام نفس المتصفح الشخصي
E-Mail	بريد منفصل أو alias مستقل	استخدام بريدك الحقيقي أو بريد مستخدم سابقًا
Phone	رقم منفصل وغير مرتبط بحساباتك	استخدام رقمك الشخصي للتحقق
Profile Details	اسم، بلد، لغة، صورة، عمر، اهتمامات	تفاصيل تشبهك أو تتناقض مع بعضها
Behavior	أسلوب كتابة، توقيت، نشاط، تفاعل	نفس نمطك الحقيقي أو نشاط غير طبيعي

لا تبني هوية مجهولة فوق آثار قديمة. ابدأ من بيئة نظيفة ومفصولة.

أخطاء شائعة

- استخدام رقم الهاتف الشخصي.
- استخدام بريد مؤقت معروف ومرفوض.
- التسجيل من نفس المتصفح الشخصي.
- استخدام Continue with Google أو Apple.
- اختيار تفاصيل حساب غير متسقة.
- إعادة استخدام نفس اسم المستخدم.
- دفع خدمة ببطاقة شخصية.
- رفع صورة وجه حقيقية.

خطأ واحد في الهاتف أو الدفع أو الصورة قد يكسر العزل كاملًا.

Email Aliasing

aliases تساعدك على عدم كشف البريد الأساسي لكل جهة. لكنها ليست بديلًا عن بريد منفصل أو بيئة تسجيل معزولة.

- استخدم alias مختلف لكل منصة.
- لا تستخدم alias مرتبط ببريدك الحقيقي للحسابات الحساسة.
- افصل بريد الهوية عن بريدك الشخصي.
- راقب أين استخدمت كل alias.
- لا تستخدم نفس alias في عدة خدمات.

البريد المنفصل + aliases أفضل من بريد واحد لكل شيء.

أسئلة فحص سريعة

- هل الرقم منفصل؟
- هل البريد منفصل؟
- هل IP مناسب وغير متناقض؟
- هل المتصفح جديد ونظيف؟
- هل الاسم واللغة والبلد متسقون؟
- هل يوجد دفع أو صورة أو حساب يربطني؟
- هل السلوك طبيعي وغير آلي؟

لا تنشئ الحساب إذا كانت إحدى الطبقات مرتبطة بك.

✅ Checklist الفصل العاشر

✓ **هل فصلت رقم الهاتف عن هويتك الحقيقية؟**

لا تستخدم رقمك الشخصي أو رقمًا مستخدمًا في حساباتك الحقيقية.

✓ **هل البريد منفصل وطويل المدى؟**

تجنب البريد المؤقت المعروف، واستخدم alias منفصل لكل خدمة عند الحاجة.

✓ **هل البيئة والمتصفح والشبكة منفصلة؟**

استخدم VM/Qube/Browser profile نظيفًا ومسار شبكة مناسبًا للهوية.

✓ **هل تفاصيل الحساب متسقة؟**

اللغة، البلد، العمر، الاسم، والصورة يجب ألا تعطي تناقضات واضحة.

✓ **هل تجنبت نقاط كسر المجهولية؟**

لا تستخدم وثائق، بطاقة دفع شخصية، وجهك، أو تسجيل دخول عبر منصة شخصية.

📝 الخلاصة النهائية للفصل

الفصل العاشر يوضح أن إنشاء هوية مجهولة عملية دقيقة وليست مجرد اسم مستعار. المنصات تستخدم التحقق بالهاتف والبريد، IP filters، البصمة، السلوك، الدفع، القياسات الحيوية، والمراجعات اليدوية لتقييم الحساب. لذلك يجب بناء الهوية كمنظومة منفصلة ومتسقة من البداية.

Takeaway: لا تسأل فقط "هل الحساب باسم مختلف؟"؛ اسأل: هل كل طبقة من الهوية — الشبكة، الجهاز، البريد، الرقم، السلوك، والدفع — منفصلة فعلًا؟

Chapter 11 • Communication, Sharing & Maintenance

الفصل الحادي عشر: التواصل، مشاركة الملفات والصيانة الآمنة

هذا الفصل يركز على ما يحدث بعد إنشاء البيئة والهوية: كيف تتواصل؟ كيف تشارك الملفات؟ كيف تنشر معلومات بشكل عام دون كشف هويتك؟ كيف تنقح الصور والمستندات؟ وكيف تحافظ على النسخ الاحتياطية والمزامنة دون أن تتحول إلى مصدر تسريب؟

6	4	3	1
محاور عملية	أنواع مشاركة	طبقات Backup	قاعدة: نظّف قبل النشر

فكرة الفصل

بعد بناء الهوية والبيئة، يصبح الخطر في التواصل والمحتوى. الرسائل، الملفات، الصور، الروابط، النسخ الاحتياطية، والمزامنة قد تكشف معلومات أكثر من الحساب نفسه.

- المحادثات قد تكشف أسلوبك أو وقتك أو علاقاتك.
- الملفات قد تحتوي Metadata أو Watermarking.
- النشر العام يحتاج مراجعة مضاعفة قبل الإرسال.
- النسخ الاحتياطي الخاطئ قد يربط البيئات ببعضها.
- المزامنة السحابية قد تكسر العزل بين الأجهزة والهويات.

الخلاصة: لا يكفي أن تكون بيئتك معزولة؛ يجب أن يكون المحتوى الذي تخرجه منها نظيفًا أيضًا.

Private Sharing & Anonymous Chat

مشاركة الملفات أو الدردشة بشكل خاص تحتاج اختيار أداة مناسبة، لكن الأداة وحدها لا تكفي. يجب الانتباه إلى التسجيل، رقم الهاتف، البريد، Metadata، وسلوك المحادثة نفسه.

الخطر

بعض أدوات المراسلة تطلب رقم هاتف أو بريدًا، وبعضها يحتفظ ببيانات وصفية أو يربطك بجهات الاتصال أو الجهاز.

Phone Link

Metadata

التخفيف

استخدم أدوات تسمح بتسجيل أقل ارتباطًا، وافتحها داخل بيئة معزولة، ولا تستخدم رقمك أو بريدك الحقيقي.

Isolation

Minimal Identity

خريطة التواصل والمشاركة

المحور	الهدف	الخطر	الممارسة الأفضل
Private Chat	تواصل مباشر مع طرف آخر	رقم هاتف، بريد، Metadata، أسلوب كتابة	أداة مناسبة + بيئة معزولة + حساب منفصل
Private File Sharing	إرسال ملف لطرف محدد	Metadata، Watermarking، سجل مشاركة	تنظيف الملف وتشفيره قبل المشاركة
Public File Sharing	نشر ملف للعامة	كشف الهوية عبر المحتوى أو المنصة أو رابط الملف	مراجعة ثلاثية، منصة مناسبة، إزالة كل المؤشرات
Redaction	إخفاء معلومات حساسة من مستند أو صورة	Blur ضعيف، طبقات قابلة للاسترجاع، Metadata	حذف/قص نهائي بدل تمويه ضعيف
Backups	حفظ العمل دون فقدان	النسخ تكشف الهوية أو تربط الأجهزة	نسخ مشفرة ومفصولة عن الحسابات الشخصية

Sync	مزامنة الملفات بين الأجهزة	ربط البيئات والهويات عبر حساب سحابي واحد	تجنب المزامنة أو استخدم تشفيرًا وفصلًا واضحًا

Public Sharing Without Identity Leaks

عند نشر ملفات أو معلومات للعامة، يجب افتراض أن كل شيء سيتم تحليله: النص، الصور، التوقيت، الرابط، المنصة، Metadata، وحتى طريقة ترتيب المعلومات. لا تنشر قبل أن تفحص المحتوى والملفات والسيناريو بالكامل.

1 Curate the Content

احذف أي معلومة شخصية، مكان، زمن، اسم، لهجة، قصة، أو تفصيل يمكن ربطه بهويتك.

2 Clean the Files

افحص Metadata، Watermarking، أسماء الملفات، خصائص المستند، والطبقات المخفية.

3 Choose the Platform

استخدم منصة مناسبة لا تتطلب حسابًا حقيقيًا أو دفعًا أو ربطًا مباشرًا بالهوية.

4 Triple Check

راجع مرة ثانية وثالثة. بعد النشر العام، قد لا تستطيع استرجاع الأثر أو حذف النسخ.

النشر العام لا يرحم. تعامل مع الملف المنشور كأنه سيُنسخ ويُحلل ويُؤرشف.

Public File Platforms

الملف يذكر خيارات مثل CryptPad وAnonArchive وFilen، مع الإشارة إلى حدود التخزين المجاني واستخدام IPFS مثل Pinata كخيار للنشر العام.

- CryptPad للتعاون والملفات.
- AnonArchive لمشاركة عامة.
- Filen كخيار تخزين.
- IPFS للنشر الموزع.
- Pinata كخدمة IPFS pinning.

المنصة لا تنظف ملفاتك. أنت مسؤول عن إزالة البيانات الكاشفة قبل الرفع.

Safe Redaction

تنقيح المستندات والصور والفيديو والصوت لا يعني وضع Blur سريع فقط. يجب إزالة المعلومة من الأصل أو قصها نهائيًا، ثم تصدير نسخة جديدة لا تحتوي طبقات قابلة للاسترجاع.

- لا تستخدم Blur ضعيف أو Pixelation لحجب معلومات مهمة.
- استخدم مربعات صلبة أو قص نهائي للمعلومة.
- صدّر نسخة جديدة بدل تعديل الملف الأصلي فقط.
- افحص Metadata بعد التنقيح.
- راجع الصوت والخلفية والانعكاسات داخل الفيديو.

Recommended Editing Approach

يفضّل استخدام أدوات مفتوحة المصدر مثل LibreOffice وGIMP وAudacity وVLC وأدوات PDF المناسبة، وتشغيلها داخل VM أو Tails لتقليل التسريبات من النظام الشخصي.

Documents

LibreOffice أو محرر نصوص بسيط، مع تصدير نسخة نظيفة وفحص Metadata.

Pictures

GIMP أو أدوات تحرير محلية، مع إزالة EXIF ومراجعة الخلفية.

- لا تستخدم أدوات تجارية مغلقة إذا كانت تضيف Telemetry أو Metadata.

التنقيح الصحيح يعني إزالة المعلومة، وليس فقط جعلها أقل وضوحًا.

Audio

Audacity لتحرير الصوت وإزالة المقاطع أو المؤشرات الصوتية الحساسة.

PDF

PDF redaction tools أو LibreOffice مع التأكد أن النص المحذوف غير قابل للاسترجاع.

الأفضل تشغيل أدوات التحرير داخل بيئة معزولة بدل جهازك الشخصي.

Communicating Sensitive Information to Organizations

إذا أردت التواصل مع منظمة معروفة مثل جهة صحفية أو حقوقية أو بحثية، لا تفترض أن الجهة ستحمي مجهوليتك تلقائيًا. يجب أن تحمي نفسك من جهتك: بيئة منفصلة، ملف نظيف، قناة مناسبة، وعدم كشف تفاصيل زائدة.

قبل التواصل	الإجراء	لماذا؟
البيئة	استخدم Tails أو Whonix أو Qubes حسب الحاجة	منع كشف الجهاز أو الشبكة الشخصية
الملفات	افحص Metadata وWatermarking وMalware	منع ربط الملف بك أو بجهة داخلية
الكتابة	راجع الأسلوب اللغوي والتفاصيل الشخصية	تقليل بصمة الكتابة والقرائن الواقعية
القناة	استخدم قناة موصى بها من الجهة نفسها إن وجدت	تقليل أخطاء النقل أو الانتحال
المخاطر	قيّم العواقب القانونية والأخلاقية والأمنية	حماية نفسك والآخرين قبل النشر أو الإرسال

لا تثق أن الطرف المستلم سيحميك. صمّم العملية كأن حماية هويتك مسؤوليتك بالكامل.

Maintenance & Secure Backups

الصيانة تعني أن البيئة لا تبقى آمنة تلقائيًا. يجب تحديث الأدوات، مراجعة الحسابات، تنظيف الملفات، وحفظ نسخ احتياطية مشفرة لا تربط الهويات ببعضها.

نوع النسخ	متى يستخدم؟	الخطر	الممارسة الأفضل
Offline Backups	ملفات حساسة أو قواعد كلمات مرور	فقدان الجهاز أو تلف التخزين	نسخ مشفرة على وسيط منفصل ومخزن بأمان
Selected Files Backups	ملفات محددة مهمة	نسيان ملفات حرجة أو نسخ Metadata	اختيار واعٍ للملفات وتنظيفها وتشفيرها
Full Disk Backups	استرجاع بيئة كاملة	نسخ آثار أو ملفات حساسة دون قصد	تشفير كامل وتخزين منفصل واختبار الاسترجاع
Online Backups	عند الحاجة للوصول عن بعد	مزود الخدمة، الحساب، Metadata، الربط	تشفير محلي قبل الرفع وعدم استخدام حساب

Online Sync Risk

المزامنة بين الأجهزة قد تكون مريحة، لكنها خطيرة في سياق المجهولية؛ لأنها قد تربط جهازًا شخصيًا ببيئة مجهولة عبر نفس الحساب أو نفس مجلد المزامنة.

- لا تستخدم حسابك السحابي الشخصي.
- لا تزامن ملفات الهوية المجهولة مع جهازك اليومي.
- شفّر محليًا قبل الرفع.
- افصل مجلدات كل هوية.
- لا تترك أسماء ملفات كاشفة.
- اختبر الاسترجاع قبل الاعتماد على النسخ.

المزامنة قد تكسر العزل بدون أن تلاحظ.

			شخصي
Information Backups	ملاحظات، كلمات مرور، مفاتيح استرداد	كشف الحسابات أو الهويات	تخزين مشفر ومنفصل مع خطة استرداد واضحة

أخطاء شائعة

- إرسال ملف أصلي دون تنظيف.
- استخدام Blur بدل إزالة حقيقية.
- رفع ملفات حساسة لسحابة شخصية.
- فتح أداة تحرير من النظام الشخصي.
- مشاركة رابط من حساب مرتبط بك.
- مزامنة ملفات مجهولة مع جهازك الحقيقي.
- نسيان Watermarking أو خصائص المستند.

أفضل ممارسات

- نظّف الملفات قبل المشاركة.
- استخدم أدوات مفتوحة المصدر قدر الإمكان.
- شغل أدوات التحرير داخل VM أو Tails.
- شفّر الملفات قبل التخزين أو النقل.
- استخدم نسخًا احتياطية Offline للبيانات الحساسة.
- راجع المحتوى ثلاث مرات قبل النشر العام.
- لا تثق بالمستلم لحماية هويتك.

كل ملف خارج بيئتك يجب اعتباره أثرًا قابلًا للتحليل.

أسئلة فحص سريعة

- هل الملف يحتوي Metadata؟
- هل توجد Watermarking؟
- هل النص يكشف أسلوبك أو حياتك؟
- هل الصورة تكشف مكانًا أو انعكاسًا؟
- هل النسخة الاحتياطية مشفرة؟
- هل المزامنة تربط هويتين؟
- هل الرابط أو الحساب يكشفك؟

لا تنشر أو ترسل قبل الإجابة بوضوح.

Checklist الفصل الحادي عشر

- ✓ **هل نظفت الملفات قبل الإرسال أو النشر؟**
  افحص Metadata، أسماء الملفات، Watermarking، وخصائص المستند.
- ✓ **هل استخدمت Redaction حقيقيًا؟**
  لا تعتمد على Blur ضعيف. احذف أو قص أو غطِّ المعلومات الحساسة نهائيًا.
- ✓ **هل راجعت المحتوى نفسه؟**
  النص، الصور، الصوت، الفيديو، التوقيت، والأسلوب قد يكشفون قرائن عنك.
- ✓ **هل النسخ الاحتياطية مشفرة ومفصولة؟**
  لا تخزن نسخ الهوية الحساسة داخل حسابك الشخصي أو جهازك اليومي.
- ✓ **هل تجنبت المزامنة التي تربط الهويات؟**
  لا تستخدم نفس السحابة أو المجلد أو الحساب بين بيئات منفصلة.

الخلاصة النهائية للفصل

الفصل الحادي عشر يوضح أن المجهولية لا تنتهي عند إنشاء الحساب أو تشغيل Tor/Whonix/Qubes. الخطر يستمر في كل رسالة، ملف، صورة، نسخة احتياطية، أو مزامنة. لذلك يجب التعامل مع التواصل والمشاركة والصيانة كجزء أساسي من OPSEC، وليس كخطوة ثانوية.

Takeaway: لا تسأل فقط "هل بيئتي آمنة؟"؛ اسأل: هل ما أرسله أو أنشره أو أخزنه يكشفني أو يربط هوياتي ببعضها؟

الفصل الثاني عشر: إزالة الآثار، المسح الآمن والخاتمة العملية

هذا الفصل يركز على المرحلة الأخيرة: ماذا يحدث بعد الاستخدام؟ كيف تتعامل مع الآثار المتبقية على الأقراص والمنصات ومحركات البحث؟ كيف تفهم الفرق بين HDD وSSD؟ ومتى يكون الحذف العادي غير كافٍ؟ الفكرة الأساسية أن إدارة الآثار جزء من OPSEC، وليست خطوة تجميلية بعد الانتهاء.

7	**2**	**3**	**1**
محاور نهائية	أنواع تخزين مهمة	مصادر آثار	قاعدة: خطط للحذف قبل الإنشاء

فكرة الفصل

الفصل الأخير لا يقول إنك تستطيع حذف كل شيء من الوجود. الفكرة الواقعية هي تقليل الآثار، فهم حدود المسح، وتنظيف ما تستطيع تنظيفه قبل أن يتحول إلى دليل أو رابط بين الهويات.

- الحذف العادي لا يعني اختفاء البيانات فعليًا.
- طريقة التعامل مع HDD تختلف عن SSD.
- محركات البحث قد تحتفظ بنسخ مؤرشفة أو cached.
- المنصات قد تسمح بالحذف أو التعديل أو تغيير الاسم.
- أفضل OPSEC هو تقليل الأثر من البداية، لا محاولة تنظيفه لاحقًا فقط.

الخلاصة: لا تبنِ خطة الخصوصية على فكرة "سأحذف لاحقًا". صمّم البيئة بحيث لا تنتج آثارًا خطيرة من الأساس.

Understanding HDD vs SSD

الأقراص الصلبة التقليدية HDD والأقراص الحديثة SSD لا تتعامل مع الحذف بنفس الطريقة. في HDD تكون الكتابة على مواقع فيزيائية أكثر مباشرة، بينما SSD يستخدم تقنيات مثل wear-leveling وTRIM وgarbage collection لتحسين الأداء والعمر.

HDD

الحذف الآمن عبر الكتابة فوق المساحة قد يكون أكثر منطقية، لأن البيانات غالبًا تقع في أماكن يمكن استهدافها بالمسح المتكرر.

Magnetic Disk

Overwrite

SSD

المسح بالكتابة فوق الملفات ليس دائمًا مباشرًا بسبب wear-leveling وTRIM. لذلك قد يكون Secure Erase أو تشفير كامل مسبقًا أفضل حسب الحالة.

TRIM

Wear-Leveling

خريطة إزالة الآثار

المصدر	نوع الأثر	المشكلة	الممارسة الأفضل
Local Disk	ملفات، Cache، Logs، Thumbnails	قد تبقى آثار حتى بعد الحذف العادي	تشفير كامل، بيئات مؤقتة، تنظيف واعٍ حسب نوع

	Temp files		القرص
HDD	بيانات قابلة للكتابة فوقها	الحذف العادي لا يمسح المحتوى فعليًا	Secure wiping أو مسح كامل عند التخلص من القرص
SSD / NVMe	بيانات موزعة بسبب wear-leveling	الكتابة فوق الملف لا تضمن الوصول لنفس الخلايا	TRIM، Secure Erase من Firmware، أو تشفير مسبق
Platforms	حسابات، منشورات، تعليقات، أسماء مستخدمين	بعض الآثار تبقى في المنصة أو لدى أطراف أخرى	حذف، تعديل، تغيير اسم، أو تقليل قابلية الربط
Search Engines	نتائج مفهرسة ونسخ cached	المحتوى قد يبقى ظاهرًا حتى بعد حذفه من الموقع	طلب تحديث أو إزالة النتائج القديمة بعد تنظيف المصدر
Backups	نسخ قديمة من ملفات أو حسابات	الحذف من الجهاز لا يحذف النسخة الاحتياطية	تشفير النسخ وإدارتها وفصلها حسب الهوية

SSD Concepts: Wear-Leveling, TRIM & Garbage Collection

فهم SSD مهم لأن كثيرًا من نصائح الحذف القديمة مبنية على HDD. في SSD، وحدة التخزين قد تنقل البيانات داخليًا لتحسين عمر الخلايا، وقد لا تعرف أنت أين أصبحت البيانات فعليًا.

1 Wear-Leveling

SSD يوزع الكتابة على خلايا مختلفة حتى لا تتلف منطقة واحدة بسرعة. هذا يجعل الكتابة فوق ملف محدد أقل وضوحًا.

2 TRIM

يخبر نظام التشغيل الـ SSD أن بعض الكتل لم تعد مستخدمة. هذا يساعد القرص على تنظيفها داخليًا.

3 Garbage Collection

عملية داخلية في SSD لإعادة تنظيم البيانات وتنظيف الكتل غير المستخدمة وتحسين الأداء.

4 Practical Limit

لا تفترض أن أداة overwrite عادية تعطي نفس النتيجة على SSD كما في HDD. نوع القرص يغيّر الاستراتيجية.

مهم: التشفير الكامل قبل الاستخدام أسهل وأقوى غالبًا من محاولة مسح آثار حساسة بعد سنوات.

Encryption First

أفضل طريقة لتقليل خطر البيانات المتبقية هي استخدام تشفير كامل من البداية. إذا كان القرص مشفرًا جيدًا، فإن التخلص من المفاتيح أو إعادة تهيئة آمنة يصبح أكثر فعالية.

- فعّل Full Disk Encryption مبكرًا.
- استخدم passphrase طويلة.
- لا تحفظ recovery keys في حسابات شخصية.
- افصل نسخ المفاتيح حسب الهوية.
- لا تعتمد على الحذف العادي للبيانات الحساسة.

التشفير قبل إنشاء البيانات أفضل من تنظيفها بعد انتشارها.

Secure Wiping: Whole Device

عندما تريد التخلص من جهاز أو قرص كامل، يجب اختيار طريقة تناسب نوع التخزين. في HDD يمكن استخدام مسح كامل بالكتابة فوق البيانات. في SSD/NVMe الأفضل غالبًا استخدام أدوات الشركة المصنعة أو خيارات Secure Erase من BIOS/UEFI إن كانت متوفرة.

- حدد أولًا هل القرص HDD أم SSD/NVMe.
- في HDD: المسح الكامل بالكتابة فوق البيانات أكثر ملاءمة.
- في SSD/NVMe: استخدم Secure Erase أو Sanitize عند توفره.
- لا تخلط بين "Format" و "Secure Wipe".
- بعد المسح، لا تعيد إدخال بيانات شخصية على نفس البيئة بلا خطة.

المسح الخاطئ قد يعطيك شعورًا زائفًا بأن البيانات اختفت.

Deleting Files Securely

حذف ملف واحد ليس دائمًا كافيًا. قد تبقى نسخ في cache، thumbnails، recent files، temporary folders، backups، cloud sync، أو داخل التطبيقات نفسها.

HDD File Deletion

قد يساعد secure delete أو free-space wipe، لكن يجب فهم حدود الأدوات.

SSD File Deletion

اعتمد على TRIM والتشفير وSecure Erase بدل overwrite العشوائي.

Application Traces

راجع recent files، cache، thumbnails، logs وtemporary folders.

Cloud Copies

الحذف المحلي لا يحذف النسخ السحابية أو النسخ الاحتياطية تلقائيًا.

القاعدة: احذف المصدر، ثم الآثار، ثم النسخ الاحتياطية، ثم افحص هل بقيت نسخة مفهرسة أو متزامنة.

Removing Traces from Search Engines & Platforms

بعض الآثار لا تكون على جهازك، بل على المنصات ومحركات البحث. قد تحذف منشورًا من موقع، لكنه يبقى ظاهرًا في نتائج البحث أو محفوظًا في cache أو في أرشيفات أو عبر screenshots عند مستخدمين آخرين.

المرحلة	ماذا تفعل؟	الهدف	الحدود
Platform Cleanup	احذف الحساب أو المنشورات إن أمكن	إزالة المصدر الأصلي	بعض المنصات لا تحذف كل شيء فورًا
Rename / Edit	غيّر الاسم والبيانات أو عدّل المنشورات القديمة	تقليل قابلية الربط	قد تبقى النسخ القديمة في الأرشيف
Search Engine Update	اطلب تحديث أو إزالة النتائج القديمة	تقليل ظهور النسخ cached	لا يزيل المحتوى من الموقع الأصلي
Data Brokers	اطلب حذف أو opt-out عند الإمكان	تقليل ظهور البيانات الشخصية	تحتاج متابعة دورية
Archived Copies	تحقق من الأرشيفات والنسخ المتداولة	فهم مدى الانتشار	قد لا يمكن حذف كل النسخ

حذف النتيجة من محرك البحث لا يعني حذف المحتوى من الإنترنت. ابدأ دائمًا بالمصدر الأصلي.

Cleanup Tools & Practical Limits

أدوات التنظيف قد تساعد في إزالة آثار محلية مثل cache وlogs وrecent files، لكنها ليست ضمانًا. يجب استخدامها بعقلية مساعدة، لا كحل سحري. الأهم هو استخدام بيئات مؤقتة، تشفير كامل، وفصل الهويات منذ البداية.

الأداة / الفكرة	الاستخدام	ملاحظة مهمة
BleachBit	تنظيف cache، logs، recent files، وبعض آثار النظام	لا تعتمد عليه وحده للبيانات الحساسة جدًا
OS Optimize / TRIM	مساعدة SSD على تنظيف الكتل غير المستخدمة	مفيد للـ SSD لكنه لا يعوض التخطيط المسبق
Secure Erase	مسح كامل للقرص عند التخلص من الجهاز	استخدم خيارًا مناسبًا لنوع القرص والشركة المصنعة
Fresh VM / Snapshot	الرجوع لحالة نظيفة بعد الاستخدام	مفيد في Whonix وQubes عند إدارة الهويات
Live OS	تقليل الآثار المحلية بعد الإغلاق	لا يمنع آثار الشبكة أو أخطاء المستخدم

Appendices Role

الملاحق في نهاية الدليل ليست فصلًا نظريًا فقط، بل مرجع سريع لموضوعات عملية مثل إعدادات Windows، المتصفحات، VPN، Tor bridges، المدفوعات، وVirtualization.

- استخدم الملاحق عند الحاجة لتفاصيل إضافية.
- لا تطبق كل شيء دفعة واحدة.
- اختر الملحق حسب المسار الذي تعمل عليه.
- راجع الملاحق عند تحديث الأدوات أو تغيير البيئة.
- اعتبرها مرجع تشغيل، لا checklist عشوائية.

الملاحق تساعدك تعالج التفاصيل بعد فهم الخطة العامة.

أخطاء شائعة

- الاعتقاد أن Delete يعني اختفاء الملف.
- استخدام نفس طريقة المسح لـ HDD وSSD.
- نسيان النسخ السحابية والاحتياطية.
- تنظيف الجهاز وترك الحسابات والمنشورات.
- الاعتماد على أداة تنظيف واحدة كحل كامل.
- نشر محتوى حساس ثم محاولة إزالته بعد انتشاره.
- عدم اختبار الاسترجاع أو فحص الآثار المتبقية.

أفضل ممارسات

- فعّل التشفير الكامل من البداية.
- استخدم VMs أو Live OS للأنشطة الحساسة.
- افصل الحسابات والملفات والنسخ الاحتياطية.
- نظف Metadata قبل النشر.
- استخدم Secure Erase المناسب عند التخلص من جهاز.
- اطلب تحديث نتائج البحث بعد حذف المصدر.
- خطط لدورة حياة الهوية من الإنشاء إلى الإغلاق.

أفضل أثر هو الذي لم يتم إنشاؤه أصلًا.

أسئلة فحص سريعة

- هل القرص HDD أم SSD؟
- هل كان القرص مشفرًا قبل الاستخدام؟
- هل توجد نسخ في cloud أو backups؟
- هل بقيت thumbnails أو recent files؟
- هل المحتوى مفهرس في محركات البحث؟
- هل الحساب قابل للحذف أو التعديل؟
- هل توجد روابط بين هذه الهوية وهويات أخرى؟

لا تعتبر التنظيف منتهيًا حتى تفحص كل الطبقات.

Final Course Map

المرحلة	الفصول	الهدف	النتيجة المطلوبة
الفهم الأساسي	CH1–CH3	Threat Model، التتبع، تسريبات الجهاز	فهم من أين تأتي المخاطر
المحتوى والسلوك	CH4–CH6	OSINT، Malware، التجهيزات العامة	تقليل أخطاء الإنسان والملفات
البيئات العملية	CH7–CH9	Tor، Tails، Whonix، Qubes	اختيار بيئة تشغيل مناسبة
الهوية والتواصل	CH10–CH11	إنشاء الهويات والتواصل والمشاركة	بناء هوية متسقة ونظيفة
الإغلاق والصيانة	CH12	إزالة الآثار والنسخ والبحث	تقليل البقايا والروابط بعد الاستخدام

Checklist الفصل الثاني عشر

- ✓ **هل فهمت نوع التخزين قبل محاولة المسح؟**
  HDD وSSD/NVMe يحتاجان استراتيجيات مختلفة للحذف والمسح.
- ✓ **هل كان القرص مشفرًا من البداية؟**
  التشفير المسبق يقلل الخطر أكثر من محاولة حذف آثار كثيرة لاحقًا.
- ✓ **هل نظفت المصدر قبل محركات البحث؟**
  احذف أو عدّل الحسابات والمنشورات أولًا، ثم اطلب تحديث نتائج البحث.
- ✓ **هل راجعت النسخ الاحتياطية والمزامنة؟**
  لا تنسَ snapshots، sync folders، cloud backups، ونسخ الأجهزة الأخرى.
- ✓ **هل أغلقت الهوية بطريقة تقلل الربط؟**
  غيّر أو احذف أو افصل البيانات التي تربط هذه الهوية بهوياتك الأخرى.

الخلاصة النهائية للفصل

الفصل الثاني عشر يختتم المقرر بفكرة مهمة: الخصوصية والمجهولية لا تنتهيان عند استخدام الأداة الصحيحة. يجب التفكير في دورة حياة كاملة: إنشاء الهوية، استخدامها، مشاركة المحتوى، النسخ الاحتياطي، ثم تنظيف الآثار وإغلاق الحسابات أو الأجهزة بشكل صحيح. كل مرحلة يمكن أن تكشفك إذا لم تكن جزءًا من الخطة.

Takeaway: لا تسأل فقط "كيف أبدأ بهوية مجهولة؟"؛ اسأل أيضًا: كيف أنهيها، أنظف آثارها، وأمنع ربطها بي لاحقًا؟

Practical Toolkit 4 • Chapters 10–12

الحزمة العملية الرابعة: بناء الهوية، المشاركة النظيفة وإغلاق الآثار

هذه الصفحة تجمع الجانب العملي من الفصول 10 إلى 12. الهدف هو تحويل خطوات إنشاء الهوية، التواصل، مشاركة الملفات، النسخ الاحتياطي، المزامنة، والتنظيف النهائي إلى Workflow واضح: قبل الإنشاء، أثناء الاستخدام، قبل النشر، وبعد إغلاق الهوية.

5	12	4	1
مراحل تشغيل	نقاط فحص	Checklists	خطة إغلاق نهائية

هدف هذه الصفحة

بعد الفصول 10–12، التركيز يصبح على دورة حياة الهوية كاملة: كيف تنشئها؟ كيف تستخدمها؟ كيف تشارك محتوى بدون تسريب؟ كيف تحفظ نسخًا آمنة؟ وكيف تغلق الهوية أو تقلل آثارها بدون أن تربطها بهويتك الحقيقية أو بهويات أخرى.

Identity Build

بريد، رقم، اسم، متصفح، شبكة، وسلوك منفصل.

CH10

Clean Sharing

تنظيف Metadata وRedaction صحيح قبل التواصل أو النشر.

CH11

Backups & Sync

نسخ احتياطي مشفر ومفصول بدون ربط الهويات.

CH11

Track Reduction

تقليل آثار الجهاز، المنصات، محركات البحث، والنسخ القديمة.

CH12

Anonymous Identity Build Checklist

قبل إنشاء أي حساب، افحص كل طبقة من طبقات الهوية. لا تبدأ التسجيل إذا كان الرقم، البريد، الجهاز، الشبكة، أو السلوك مرتبطًا بك.

- ✓ **بريد منفصل**
  لا تستخدم بريدك الحقيقي أو بريدًا مستخدمًا في حساباتك الشخصية.
- ✓ **رقم منفصل عند الحاجة**
  تجنب رقمك الشخصي؛ رقم الهاتف من أقوى روابط الهوية.
- ✓ **بيئة تسجيل نظيفة**
  استخدم VM أو Qube أو متصفحًا منفصلًا حسب مستوى التهديد.

Identity Consistency Matrix

الهوية غير المتسقة ترفع الشك: بلد مختلف، لغة غير منطقية، توقيت نشاط متناقض، IP غريب، بريد مؤقت، وسلوك آلي.

العنصر	ما يجب فحصه
Country	هل البلد يناسب اللغة والـ IP وبيانات الحساب؟
Language	هل أسلوب الكتابة ثابت وغير قريب من هويتك الحقيقية؟
Time Zone	هل وقت النشاط لا يكشف مكانك الحقيقي؟
Browser	هل البصمة نظيفة وغير مميزة جدًا؟
Behavior	هل النشاط طبيعي وليس سريعًا أو آليًا؟

لا تعالج الربط بعد إنشاء الحساب. افصل الطبقات قبل أول تسجيل دخول.

📊 Full Operational Workflow

المرحلة	الإجراء العملي	الفحص المطلوب	خطأ خطير
قبل الإنشاء	جهّز البريد، الرقم، البيئة، المتصفح، ومسار الشبكة	هل كل طبقة منفصلة؟	استخدام بريد أو رقم شخصي
أثناء التسجيل	استخدم بيانات متسقة ولا تربط بحسابات خارجية	هل البلد واللغة والـ IP منطقية؟	Continue with Google / Apple / Facebook
أثناء الاستخدام	حافظ على سلوك طبيعي ومنفصل	هل الأسلوب أو التوقيت يكشفك؟	إعادة استخدام نفس الاسم أو أسلوب الكتابة
قبل المشاركة	نظّف الملفات والصور والمستندات	هل Metadata وWatermarking أُزيلت؟	نشر ملف أصلي من جهازك
قبل النسخ الاحتياطي	شفّر الملفات وافصلها عن حساباتك الشخصية	هل النسخة مشفرة ومفصولة؟	رفعها إلى cloud شخصي
عند الإغلاق	احذف أو عدّل أو افصل الحسابات والملفات والنتائج	هل بقيت نسخ أو نتائج بحث؟	حذف الحساب ونسيان النسخ الاحتياطية

📂 Clean File Sharing Toolkit

قبل إرسال أو نشر أي ملف، نظفه كأن شخصًا سيحلله جنائيًا. افحص الاسم، الخصائص، Metadata، المحتوى، الخلفية، الطبقات، والنسخ السابقة.

ExifTool
فحص وإزالة Metadata من الصور والمستندات وأنواع متعددة من الملفات.

MAT2
Metadata Anonymisation Toolkit لإزالة البيانات الوصفية محليًا.

GIMP
تحرير الصور محليًا مع قص أو تغطية المعلومات الحساسة بشكل صحيح.

Audacity
تحرير الصوت وإزالة المقاطع أو المؤشرات الصوتية الحساسة.

لا تستخدم Blur ضعيف. احذف أو قص أو غطّ المعلومة الحساسة نهائيًا.

💬 Communication OPSEC

التواصل قد يكشفك من خلال القناة، الحساب، الأسلوب، التوقيت، الملفات، أو تفاصيل زائدة داخل الرسائل.

✓ قناة مناسبة
استخدم قناة لا تتطلب رقمك أو بريدك الحقيقي عند الحاجة للعزل.

✓ رسالة قليلة القرائن
لا تذكر تفاصيل شخصية أو أماكن أو تواريخ دقيقة بلا ضرورة.

✓ ملفات نظيفة
لا ترسل مرفقات قبل إزالة Metadata وفحص المحتوى.

التواصل الآمن يعني قناة مناسبة + محتوى قليل القرائن + ملفات نظيفة.

Backup & Sync Decision Table

الحالة	الخيار الأفضل	لماذا؟	تجنب
كلمات مرور وهوية حساسة	نسخة مشفرة Offline	تقلل تسريبات cloud والمزامنة	رفع قاعدة كلمات المرور إلى حساب شخصي
ملفات عمل مجهولة	مجلد مشفر منفصل	يحافظ على فصل الهوية	خلطها مع Documents الشخصي
ملفات تحتاج وصولًا من عدة أجهزة	تشفير محلي قبل الرفع	يقلل ثقة مزود السحابة	مزامنة خام بدون تشفير
ملفات مؤقتة أو مشبوهة	DisposableVM أو بيئة مؤقتة	تقلل بقاء الآثار	نسخها إلى جهازك اليومي
أرشيف طويل المدى	تشفير + تسمية غير كاشفة + تخزين منفصل	يسهل الاسترجاع دون كشف الهوية	أسماء ملفات تكشف الموضوع أو الشخص

Track Reduction Workflow

إزالة الآثار لا تكون خطوة واحدة. ابدأ بالمصدر، ثم المنصات، ثم محركات البحث، ثم النسخ الاحتياطية، ثم الجهاز المحلي. لا تفترض أن حذف ملف أو حساب يحذف كل النسخ.

الترتيب	الطبقة	الإجراء
1	المصدر الأصلي	احذف أو عدّل أو قلل المعلومات الكاشفة من الموقع أو الحساب.
2	المنصة	راجع الحساب، المنشورات، التعليقات، الصور، أسماء المستخدمين.
3	محركات البحث	اطلب تحديث أو إزالة النتائج القديمة بعد تنظيف المصدر.
4	النسخ الاحتياطية	راجع cloud، snapshots، sync folders، وأجهزة أخرى.
5	الجهاز المحلي	نظف logs، temp، thumbnails، recent files، cache، أو استخدم بيئة جديدة.

حذف النتيجة من محرك البحث لا يحذف المحتوى من المصدر. ابدأ بالمصدر أولًا.

Storage Cleanup

طريقة التنظيف تعتمد على نوع التخزين. لا تتعامل مع HDD وSSD بنفس الأسلوب.

- اعرف نوع القرص أولًا: HDD أو SSD/ NVMe.
- فعّل التشفير الكامل مبكرًا.
- لا تعتمد على Delete أو Format سريع.
- في SSD، افهم TRIM وSecure Erase.
- في HDD، المسح بالكتابة فوق البيانات قد يكون مناسبًا.
- لا تنسَ النسخ الاحتياطية والسحابة.

التشفير قبل إنشاء البيانات أفضل من محاولة مسحها لاحقًا.

Common Failure Modes

High-Value Practices

Quick Final Questions

- إنشاء هوية ببريد أو رقم شخصي.
- استخدام نفس المتصفح لأكثر من هوية.
- إرسال ملفات أصلية دون تنظيف.
- استخدام Blur ضعيف للمعلومات الحساسة.
- النسخ الاحتياطي على cloud شخصي.
- حذف الملف المحلي ونسيان النسخ الأخرى.
- إغلاق الحساب دون تنظيف نتائج البحث.
- نسيان أن الأسلوب والسلوك قد يكشفان الهوية.

- ابن الهوية قبل استخدامها.
- افصل البريد والرقم والجهاز والشبكة.
- نظّف كل ملف قبل إرساله أو نشره.
- استخدم Redaction حقيقيًا لا Blur ضعيفًا.
- شفّر النسخ الاحتياطية محليًا.
- استخدم أسماء ملفات غير كاشفة.
- خطط لإغلاق الهوية منذ البداية.
- راجع الآثار دوريًا.

العزل الجيد لا يعتمد على خطوة واحدة، بل على اتساق كل الطبقات.

- هل هذا الحساب مرتبط برقم أو بريد حقيقي؟
- هل بيئة التسجيل نظيفة؟
- هل الملف الذي سأرسله نظيف؟
- هل الصورة تكشف مكانًا أو انعكاسًا؟
- هل النسخة الاحتياطية مشفرة؟
- هل المزامنة تربط هويتين؟
- هل حذف المصدر أم فقط النتيجة؟
- هل بقيت آثار في جهاز أو cloud؟

إذا كانت الإجابة غير واضحة، لا تنشر ولا ترسل ولا تغلق قبل الفحص.

✅ Final Checklist: Chapters 10–12

✓ هل كل طبقة في الهوية منفصلة؟

البريد، الرقم، المتصفح، الجهاز، الشبكة، السلوك، والدفع.

✓ هل المحتوى الذي ستنشره نظيف؟

افحص النص، الصورة، الصوت، الفيديو، Metadata، أسماء الملفات، والخلفيات.

✓ هل النسخ الاحتياطية لا تربط الهويات؟

لا تستخدم حساب cloud شخصي أو مجلد sync مشترك بين هويتين.

✓ هل تعرف مكان كل أثر؟

الجهاز، المنصة، محركات البحث، backups، snapshots، cloud، ورسائل التواصل.

✓ هل لديك خطة إغلاق للهوية؟

تعديل أو حذف الحساب، تنظيف النتائج، مراجعة النسخ، وتقليل الروابط المتبقية.

Final Rule: لا تنشئ أثرًا لا تعرف كيف ستتعامل معه لاحقًا.

📝 الخلاصة العملية النهائية

Practical Toolkit 4 يغلق الدورة العملية للمقرر: الهوية لا تبدأ باسم مستعار فقط، ولا تنتهي بحذف الحساب فقط. يجب أن تفكر في الهوية كدورة حياة كاملة: إنشاء، استخدام، تواصل، مشاركة، نسخ احتياطي، تنظيف، ثم إغلاق. أي طبقة مهملة قد تربط كل شيء ببعضه.

Takeaway: الهوية المجهولة الناجحة ليست التي تخفي IP فقط؛ بل التي تفصل كل طبقة وتنتج أقل قدر ممكن من الآثار القابلة للربط.