Parte 1: Le Fondamenta - L'Igiene Digitale di Base

Queste sono le pratiche essenziali, come lavarsi i denti per l'igiene personale. Senza di queste, qualsiasi altra protezione sarà inefficace.

1. Le Password: La Tua Prima Linea di Difesa

Una password debole è come lasciare la chiave di casa sotto lo zerbino.

- **Cosa Fare:**
    - **Lunghezza e Complessità:** Usa password **lunghe** (almeno 12 caratteri) che includano lettere (maiuscole e minuscole), numeri e simboli (`!@#$%^&*`). Evita sequenze comuni come "123456" o "password".
    - **Unicità: Usa una password diversa per ogni account.** Se un sito viene violato, i criminali proveranno quella stessa combinazione email/password su altri servizi (banche, social network, email). Questo si chiama "credential stuffing" ed è estremamente comune.
    - **Password Manager:** Ricordare decine di password complesse è impossibile. La soluzione è un **Password Manager**. È un programma che crea, memorizza e inserisce automaticamente password fortissime per te. Tu dovrai ricordare solo una password principale, quella per accedere al manager stesso.
        - **Esempi: LastPass**, **Bitwarden** (ottimo e gratuito), **1Password**, **KeePass**.
    - **Come Installare un Password Manager:**
        - Vai sul sito web del password manager scelto (es. bitwarden.com).
        - Crea un account gratuito.
        - Installa l'estensione per il tuo browser (Chrome, Firefox, Safari, ecc.).
        - Installa l'app sul tuo smartphone.
        - Inizia a importare o cambiare le password dei tuoi account uno per uno. Il manager ti aiuterà a generarne di nuove e robuste.

2. L'Autenticazione a Due Fattori (2FA o MFA): Il Secondo Lucchetto

Anche con una password forte, se viene rubata, l'account è compromesso. L'2FA aggiunge un secondo step di verifica, come un codice temporaneo che ricevi sul telefono.

- **Cosa Fare:**
    - **Attivala SEMPRE** dove disponibile: email, social network, home banking, cloud.
    - **Preferisci un'App Authenticator:** Anziché ricevere i codici via SMS (che possono essere intercettati), usa app come **Google Authenticator**, **Microsoft Authenticator** o **Authy**. Queste app generano codici offline sul tuo dispositivo.
    - **Come Configurare l'2FA:**
        1. Vai nelle impostazioni di sicurezza del tuo account (es. Google, Facebook).

2. Cerca "Autenticazione a due fattori" o "Two-Factor Authentication".
3. Segui la procedura per scansionare un QR code con la tua app Authenticator.
4. Inserisci il codice generato dall'app per confermare. Da quel momento, ad ogni accesso, oltre alla password, dovrai inserire il codice temporaneo.

3. Aggiornamenti Software: La Tua Armatura Senza Falle

System operativo, browser, programmi: gli aggiornamenti spesso contengono "patch" per vulnerabilità scoperte di recente. I criminali sfruttano proprio queste falle nei software non aggiornati.

- **Cosa Fare:**
  - **Abilita gli aggiornamenti automatici** su Windows, macOS, smartphone (iOS/Android).
  - **Aggiorna regolarmente le tue app**, soprattutto il browser e i plugin come Adobe Flash (ormai poco usato) o PDF Reader. Meglio ancora, usa alternative più sicure come i visualizzatori PDF integrati nei browser moderni.

Parte 2: Riconoscere le Minacce - Diventa un Cacciatore di Phishing

La tecnologia da sola non basta. La difesa più importante sei tu e la tua capacità di riconoscere un tentativo di truffa.

1. Phishing e Smishing: La Pesca di Dati via Email e SMS

L'obiettivo è ingannarti per rubare dati personali, credenziali di accesso o installare malware.

- **Come Riconoscerlo:**
  - **Urgenza e Paura:** Messaggi che creano panico ("Il tuo account sarà bloccato!", "Hai vinto un premio, clicca ora!").
  - **Mitigatore Sbagliato:** L'email sembra di Poste Italiane, ma l'indirizzo del mittente è `poste-info@serviziclientitk.com`.
  - **Errori Grammaticali:** Testi pieni di errori sono un campanello d'allarme.
  - **Link Sospetti:** Passa il mouse sopra un link (senza cliccare!) per vedere l'URL vero e proprio. Corrisponde al nome del sito che dovrebbe essere?
  - **Allegati Inaspettati:** Non aprire mai allegati (come .exe, .zip, .doc) da mittenti sconosciuti o inaspettati.
- **Cosa Fare:**
  - **Non cliccare link negli SMS/Email.** Se l'email dice che c'è un problema con il tuo account Amazon, apri manualmente il browser e vai su amazon.com per controllare.
  - **Segnala il phishing:** La maggior parte dei client email (Gmail, Outlook) ha un pulsante "Segnala come phishing".

2. Malware e Ransomware: Il Sequestro dei Tuoi Dati

Il malware è un software malevolo che si installa sul tuo dispositivo. Il ransomware è un tipo di malware che cripta tutti i tuoi file e chiede un riscatto per riaverli.

- **Come Proteggerti:**
    - **Antivirus/Antimalware:** Usa un software di sicurezza affidabile. Windows 10 e 11 includono **Windows Defender**, che è già un ottimo antivirus integrato. Per una protezione aggiuntiva, puoi considerare soluzioni come **Malwarebytes** (per scansioni periodiche).
    - **Backup, Backup, Backup!** Questa è l'arma definitiva contro il ransomware. Se hai una copia di sicurezza dei tuoi dati, puoi formattare il computer e ripristinarli senza pagare il riscatto.
        - **Come Fare un Backup:**
            - **Regola 3-2-1:** Avere **3** copie dei dati, su **2** supporti diversi (es. disco esterno + cloud), di cui **1** conservata fuori casa (es. cloud o disco a casa di un familiare).
            - **Soluzioni:** Usa un **disco rigido esterno** per backup automatici con strumenti integrati (Cronologia File su Windows, Time Machine su Mac) e un servizio di **cloud storage** come **Google Drive**, **Dropbox** o **Backblaze** per i file più importanti.

Parte 3: Protezioni Avanzate - Alzare l'Asta della Sicurezza

Una volta padroneggiate le basi, puoi implementare queste strategie per una protezione di livello superiore.

1. Reti Private Virtuali (VPN)

Una VPN cripta tutto il traffico internet tra il tuo dispositivo e un server remoto. È utilissima quando sei connesso a reti Wi-Fi pubbliche (aeroporto, bar, hotel), che sono spesso poco sicure e possono essere usate per intercettare i tuoi dati.

- **Come Sceglierne Una:**
    - Opta per servizi a pagamento con una politica "no-log" (non registrano la tua attività). Evita le VPN gratuite, che spesso monetizzano vendendo i tuoi dati.
    - **Esempi: ExpressVPN**, **NordVPN**, **ProtonVPN** (ha un piano gratuito molto rispettabile).

2. Crittografia End-to-End (E2EE)

Significa che solo tu e il destinatario potete leggere i messaggi. Nemmeno la compagnia che fornisce il servizio può accedervi.

- **Dove Usarla:**

- **Messaggistica:** Usa app come **WhatsApp**, **Signal** o **Telegram** (solo per le chat "secret") invece degli SMS.
- **Cloud Storage:** Servizi come **Tresorit** o **Sync.com** offrono crittografia E2EE per i tuoi file nel cloud.

3. Navigazione Consapevole e Privacy

- **Estensioni del Browser:** Installa estensioni come **uBlock Origin** (blocco pubblicità e tracker) e **Privacy Badger** (blocca i tracker invisibili che seguono la tua navigazione).
- **Attenzione ai Permessi delle App:** Quando installi un'app sullo smartphone, controlla quali permessi chiede. Perché un'app per le note ha bisogno di accedere alla tua posizione e ai tuoi contatti?
