Newsletter n.1

LA SICUREZZA DEI PROPRI DEVICES: COMPUTER, TABLET E CELLULARE

L'argomento sicurezza Internet si può dividere in quattro parti: protezione dei devices e della rete di casa, password, browser, navigazione su reti wifi.
Per ciascuna di queste categorie vedremo tutto quello che si dovrebbe fare per avere un livello di sicurezza minimo fino a blindare completamente il sistema ed ogni dato trasferito sul web ed in rete.

1) **Sicurezza del computer, tablet o cellulare**

E' stato installato un antivirus? L'antivirus si aggiorna automaticamente ogni giorno?
Se non è stato ancora installato un antivirus oppure se si ha un programma scaduto che non si aggiorna più, bisogna prendere provvedimenti.
Disinstallare l'antivirus attuale e scaricare uno degli antivirus gratuiti consigliati. Per giudicare un antivirus in maniera comprensibile da tutti dobbiamo tenere in considerazione almeno 6 parametri prima di prendere qualsiasi decisione. Un buon antivirus infatti:

- Non deve rallentare troppo il PC ed essere leggero in memoria RAM.
- Deve fermare i virus prima che essi possano agire (scansione attiva residente).
- Non deve rilevare troppi falsi positivi, vedendo minacce dove invece non ci sono.
- Non deve far durare troppo la scansione su richiesta o la scansione automatica periodica: un moderno SSD deve essere scansionato completamente in meno di 2 ore.
- Deve aggiornarsi automaticamente in modo da poter fermare subito le nuove infezioni e impedire l'accesso alle parti vitali del sistema.
- Deve riuscire a bloccare i malware non ancora scoperti (minacce 0-day), intuendo la minaccia sol per il comportamento sospetto di alcune componenti.

Oltre a questi parametri, tutti molto importanti quando si parla di antivirus, dobbiamo considerare anche la facilità di utilizzo, l'interfaccia utente, eventuali problemi di usabilità e la presenza di bug, errori e incompatibilità.

- **E' installato un firewall?**

Se si ha Windows 7 e se si naviga in internet usando un router a casa, non è necessario un programma firewall. Se si avesse bisogno, si può scaricare un firewall gratuito per proteggere la rete e bloccare intrusioni.

- **Windows (o Mac) è aggiornato e si aggiorna automaticamente e regolarmente?**

Molti trascurano o dimenticano di aggiornare Windows con le patch che Microsoft distribuisce ogni settimana. Tali aggiornamenti sono sempre patch di sicurezza che vanno a coprire gli ultimi buchi scoperti che permettono a utenti malintenzionati di entrare nei pc dall'esterno e prenderne il controllo.
Verificare che il servizio Windows Update sia attivo dal Pannello di Controllo.
Anche chi usa il Mac non deve assolutamente sottovalutare gli aggiornamenti di sicurezza.

- **Hai impostato un piano di backup dei dati, dei documenti e delle foto?**

Per la sicurezza di non perdere i file creati e salvati sul computer, pianificare il backup automatico così da poterne avere una doppia copia di sicurezza.
Se non si hanno troppi dati di cui fare il backup, può essere molto più facile e veloce fare un backup online sui servizi di archiviazione cloud come Dropbox e Skydrive.

- **Tieni aggiornati i programmi installati sul computer?**

Come per Windows, anche per i programmi escono spesso aggiornamenti di sicurezza.
Per chi vuole, ci sono modi per aggiornare automaticamente programmi e software installati sul computer.

- **Quando scarichi programmi, stai attento, nella procedura di installazione a non installare anche altri software "consigliati"?**

Purtroppo, molti programmi gratis sono accompagnati da sponsor, cosiddetti **"crapware",** sotto forma di programmi non richiesti che si installano automaticamente.

2) Sicurezza del browser

Il fatto che il computer, tablet o cellulare sia protetto da virus e da intrusioni esterne non garantisce che la navigazione sia comunque sicura e privata. Molte persone possono non preoccuparsi della privacy, ma la sicurezza resta comunque fondamentale.
Qualsiasi sia il browser, questo deve essere aggiornato all'ultima versione e mantenere gli aggiornamenti automatici abilitati. I browser aggiornati e con aggiornamenti automatici sono sicuramente Chrome, Firefox, Opera e Microsoft Edge.

- **Quando fai la login con password ad un sito, controlli sempre che l'indirizzo inizi con https?**

HTPPS è il protocollo della connessione cifrata e si differenzia rispetto il normale http per il fatto che ogni dato trasmesso in https è crittografato. Questo significa che quanto viene scritto in https è illegibile per chiunque, compresi i gestori di quel sito.
L'estensione per il browser HTTPS Everywhere evidenzia i siti sicuri e assicura che si stia sempre in HTTPS ove disponibile (vedi articolo Navigare in https su siti bancari, negozi online, Facebook con connessione protetta).

- **Sai riconoscere, a occhio, i siti pericolosi in cui bisogna stare attenti a dove si clicca?**

Se non si riesce ancora a distinguere un sito buono da uno cattivo a occhio e si ha sempre la paranoia o la malafede verso ogni sito diverso da quelli più famosi, allora si possono installare alcune estensioni come WOT per evitare di cliccare link pericolosi e siti sospetti

- **Quando ti colleghi ad un sito da un computer non usato solo da te, esci sempre dall'account?**

Ricordare sempre di eseguire il logout di tutti gli account che si usano su un computer pubblico o condiviso con altre persone, familiari compresi.

- **Conosci le basi delle truffe e le frodi online?**

Sapere cosa sono il phishing, i malware e altri pericoli su internet è importante per stargli alla larga.

- **Proteggi il browser dal tracciamento online?**

Come già spiegato, non farsi tracciare online dai siti significa bloccare la raccolta di dati. Questo è possibile tramite alcune estensioni da installare sul browser.

Il livello massimo di protezione e privacy su internet è la navigazione anonima. Navigare in modo completamente anonimo non è utile a tutti e non si può fare per qualsiasi situazione. Può rivelarsi utile quando si sta facendo qualcosa di illegale (ma buono come scaricare i torrent), quando non si vuole condividere la propria posizione geografica o quando si vuol falsificare l'indirizzo IP per accedere a siti bloccati.

Anche se si può navigare anonimi su internet in diversi modi, la privacy online è garantita solo con TOR browser.

3) **Sicurezza delle password usate online**

- **Usi password complesse?**

Una degli errori più frequenti tra i navigatori su internet è di usare password semplici o che rimandano a fatti o eventi della vita personale.
Bisogna sempre scegliere password impossibili da scoprire e, soprattutto, generare una password forte per tutti i siti web, senza dare possibilità a nessuno di poterla indovinare (mai usare la data di nascita, la squadra del cuore o il nome della moglie o del cane).

- **Usi password diverse per ogni sito?**

Non bisogna mai riutilizzare la stessa combinazione e-mail e password di combo in più servizi perché se un hacker riesce ad entrare in quell'account Email, potrà violare ogni account personale senza fatica.
Per gestire le diverse password basta usare un programma per creare e gestire password degli account web.
Dove possibile (Dropbox, Google, Gmail e Facebook) si può usare l'autenticazione a due fattori.
Per una maggiore protezione, assicurarsi di controllare le autorizzazioni alle app su Facebook e Twitter.

4) **Sicurezza di rete**

- **La tua rete Wifi di casa è protetta con chiave WPA2?**

Se non lo fosse o se non si ha idea di cosa sia WPA2 bisogna sapere che WPA significa Wi-Fi Protected Access e che, il Wi-Fi Protected Access II (WPA2) e il Wi-Fi Protected Access III (WPA3) sono tre protocolli di sicurezza e programmi di certificazione di sicurezza sviluppati dalla Wi-Fi Alliance per proteggere le reti di computer wireless.

- **Sei consapevole che quando ti colleghi ad una rete wifi aperta, tutto quello che fai è visibile dall'esterno del tuo computer?**

L'unica cosa che protegge la sicurezza delle password su internet in una rete wifi pubblica è il protocollo HTTPS citato nella prima domanda del punto due.

- **Hai controllato le cartelle condivise sul computer?**

Come dimostrato, entrare nei pc e vedere le cartelle condivise di altri computer è facilissimo. Molto spesso l'operazione ha successo perché la gente dimentica di escludere la condivisione di cartelle o dell'intero hard disk sul computer. Per usare un computer in completo anonimato e collegarsi in rete senza lasciare tracce, si può usare un sistema Linux anonimo e privato come Tails.

La sicurezza è importante per tutti, dal tecnico esperto all'analfabeta informatico. Il livello delle precauzioni da prendere è a propria discrezione, ma tenere a mente che oggi la sicurezza online è altrettanto importante (se non di più) della sicurezza della propria casa.

Questo progetto è stato finanziato con il sostegno della Commissione europea. Il presente documento riflette esclusivamente il punto di vista dei partner del progetto e la Commissione non può essere ritenuta responsabile per l'uso che può essere fatto delle informazioni in esso contenute.