NEWSLETTER n. 2

Quali sono i pericoli di Internet da conoscere e da cui guardarsi?

I pericoli di Internet di cui essere consapevoli, da cui guardarsi e da affrontare quando necessario possono essere racchiusi in 9 grandi categorie.

1) Siti con malware e virus pronti a infettare il vostro computer.

Quando si naviga in Internet, è molto facile cliccare sul link sbagliato e aprire un sito che carica malware sul computer. Fortunatamente, se sul vostro PC è installato un antivirus aggiornato, questo virus verrà quasi sempre bloccato prima che possa fare danni. Il pericolo maggiore, oltre a quello di un antivirus che lascia erroneamente passare il virus, è quello di non rendersi conto di aver rischiato un'infezione che potrebbe compromettere il funzionamento del PC o l'integrità dei dati. È proprio a causa della mancanza di attenzione da parte di molti che nell'ultimo anno si sono diffusi virus ransomware come Cryptlocker, che criptano i file personali e chiedono un riscatto.

Sappiamo quali sono i siti pericolosi, in genere quelli che si occupano di pirateria, siti di streaming, contenuti per adulti, incontri e materiale illegale. Se non potete evitare di visitare questo tipo di siti, fate molta attenzione a dove cliccate perché il virus può nascondersi ovunque. Basta cliccare sul pulsante "Download" sbagliato per finire con l'installare il malware. E non dimenticate quei banner pubblicitari che vi dicono che il vostro PC è infetto, quando in realtà non lo è.

In caso di dubbio, esistono strumenti per riconoscere ed evitare i link pericolosi e i siti sospetti.

Un fattore chiave per riconoscere ed evitare i siti con virus è l'utilizzo di un browser aggiornato e protetto da tutti i bug finora scoperti.

Tra i siti più pericolosi che possono contenere malware ci sono sicuramente i siti per adulti, i siti di pirateria di qualsiasi tipo, quasi tutti i siti di torrent (anche di pirateria), i siti di download illegale (come film e musica) e i siti di cracking.

Idealmente, se si deve necessariamente visitare un sito di questo tipo, sarebbe meglio navigare utilizzando una sandbox. Sia in Windows 10 che in Windows 11 è possibile utilizzare una funzione di desktop virtuale che non è solo uno strumento di sicurezza, ma anche un ottimo modo per eseguire operazioni sul computer senza che vengano registrate o ricordate, un po' come la modalità in incognito dei browser web. Questo strumento si chiama Sandbox ed è inteso come una zona del computer in cui tutto ciò che viene fatto non ha alcuna influenza sul sistema e viene cancellato immediatamente dopo la chiusura. La Sandbox funziona come una macchina virtuale usa e getta in cui è possibile eseguire in sicurezza tutto ciò che si desidera; si può persino aprire un virus o un malware senza preoccuparsi che danneggi il PC o che rubi i dati dal computer.

2) La privacy online è sempre in pericolo

È evidente che se si vuole utilizzare Internet in modo partecipativo, cioè iscrivendosi a forum, social network e chat, si deve sacrificare una parte della propria privacy. Su siti come Facebook, si è obbligati a

fornire il proprio nome reale, mentre su altri siti è ancora necessario lasciare un indirizzo e-mail attraverso il quale si può, se lo si desidera, rintracciare il proprietario. In sostanza, nel normale utilizzo di Internet, l'anonimato non può esistere e se qualcuno fosse interessato a sapere chi siamo e avesse le giuste capacità di hackeraggio e il giusto talento, potrebbe teoricamente sapere tutto di noi.

Proteggere la privacy online, tuttavia, non significa impedire a un hacker di spiare le nostre vite perché, a meno che non siamo perseguitati da uno stalker o non stiamo facendo cose illegali che devono essere nascoste, diciamo che è probabile che nessuno perda il suo tempo a entrare nelle nostre vite. La privacy online, invece, significa mantenere riservate alcune informazioni sensibili, come i numeri delle nostre carte di credito, le nostre password, dove ci troviamo in un determinato momento, cosa stiamo cercando su Internet e così via.

3) Siti non protetti

Si tratta di un fattore di pericolo che viene ancora ignorato dalla maggior parte delle persone.

I siti web non sono tutti uguali e si dividono in siti sicuri, dove le informazioni trasmesse sono criptate e non possono essere intercettate dall'esterno, e siti normali che trasmettono in chiaro. Navigaweb.net è attualmente un sito non criptato, il che non significa che non sia sicuro, ma poiché non richiede una password per accedere, non ha bisogno di proteggere le informazioni. Tutti i siti in cui è necessario inserire una password devono essere criptati, e questa protezione è riconoscibile dal lucchetto sull'indirizzo Internet e dal prefisso https anziché http. Quando un sito è in HTTPS e non presenta errori di certificato, tutte le informazioni che inviamo, comprese le password di accesso, i numeri di carta di credito o di conto corrente, non sono visibili su Internet a nessuno, nemmeno al gestore del sito a cui inviamo queste informazioni. Va da sé che su tutti i siti con http e senza https non si devono condividere informazioni personali.

Se state ancora utilizzando un servizio di posta elettronica non https o un servizio di online banking così superficiale, cambiate immediatamente.

4) Phishing

Amongst dangerous sites in general, a particular category is that of scam sites such as unknown and unrecommended shopping sites or, worse, fake sites that look identical to famous sites and are created to steal passwords for accounts.

Making fake sites copies of banking or shopping sites is one of the most common techniques used by hackers to steal web account passwords and is called Phishing. Phishing always works by sending a message via email, Facebook, SMS, Whatsapp, etc. The best way not to fall for this technique is to use it as an excuse to steal passwords. The best way to avoid falling into this kind of trap is to never write down passwords and important data (even via email) except on the official websites of the accounts, recognisable by the address written at the top of the browser and the HTTPS with green padlock.

Ideally, it would be better to use an email client such as Microsoft Outlook and use a spam filter to block these messages.

5) Spam

l pericolo dello spam è oggi molto più basso rispetto a qualche anno fa.

Per spam si intende l'intera categoria di messaggi spazzatura, pubblicità, phishing e virus o comunicazioni inutili. Fortunatamente, oggi i migliori servizi di posta elettronica, come Gmail e Outlook.com, dispongono di un efficace filtro antispam che regola la ricezione delle e-mail.

6) Misinformation

Anche se può rientrare nella categoria Spam, la disinformazione su Internet è diventata un pericolo reale nell'ultimo anno a causa della diffusione di fake news da parte di siti di bufale che dobbiamo imparare a riconoscere per non sembrare degli imbecilli che credono a qualsiasi cosa leggano su Internet o su Facebook.

7) Incontri online

Questo è uno dei pericoli più gravi di Internet per i giovani.

Sembra brutto da dire, ma un genitore responsabile dovrebbe controllare se i propri figli chattano con estranei via Internet, in qualsiasi circostanza. È possibile chattare con uno sconosciuto in un gioco online, in un sito di incontri occasionali, in un social network, in un forum e in qualsiasi altra chat room. Che sia per motivi sessuali, di incontri o puramente ricreativi, è importante non dare troppe informazioni personali: non dire la propria età reale, non dire dove si vive, non dire che scuola si frequenta, non dare i nomi reali di familiari o amici e non dare il proprio numero di telefono. I predatori online sono molto bravi a farsi passare per ragazzi normali e sanno sfruttare le debolezze degli adolescenti come nemmeno i migliori psicologi, spinti, nei casi più gravi, da quella terribile malattia che è la pedofilia

8) Cyberbullying

Chattare con gli sconosciuti può essere pericoloso perché non si sa mai chi c'è dietro la tastiera, ma anche chattare o messaggiare con persone conosciute può essere pericoloso. Il cyberbullismo funziona più o meno così: se si viene presi in giro a scuola o dai propri amici, uno di loro può pubblicare un video o una foto su Facebook o su altri siti di social network che può mettere in imbarazzo la vittima.

Un altro caso di cyberbullismo può derivare da messaggi anonimi che insultano pesantemente la vittima, anche con minacce.

Rispetto al bullo reale, il cyberbullo ha il vantaggio di non avere alcun controllo e di poter dire tutto ciò che vuole senza guardare in faccia la vittima, o addirittura in modo anonimo, nascondendosi dietro la tastiera. In entrambi i casi, non sarebbe così difficile, almeno a livello tecnico. È molto più complicato, invece, difendersi a livello psicologico, il che può richiedere l'aiuto di un genitore o di un esperto.

Per cominciare, tuttavia, sarebbe un ottimo passo avanti cancellare l'account su Ask.fm, uno dei siti che più si presta al cyberbullismo online.

9) Totale ignoranza della sicurezza informatica

Si tratta di un pericolo evidente, talmente diffuso da sorprendere.

È possibile che ancora oggi la password più comune al mondo sia 123456?

Le persone pensano che, non avendo nulla da nascondere, nessun hacker possa rubare il loro account?

Come è possibile che la gente usi ancora la stessa password per ogni sito web?

E poi c'è ancora chi scrive le proprie password, magari tutte diverse e difficili da ricordare, su un pezzo di carta che può essere letto da chiunque?

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.