Autodifesa digitale

I computer, Internet, gli smartphone,... tendono a prendere sempre più spazio nelle nostre vite. Il digitale sembra spesso molto semplice e rapido ma gli elementi di semplificazione della nostra vita non rappresentano sempre e solo dei vantaggi.

Basta essere paranoici: io non ho niente da nascondere!

Al di fuori delle casistiche più classiche come i furti di account o di dati specifici (come ad esempio quelli di una carta di credito), ci sono altri dati che potresti voler nascondere in quanto personali e riservati.

Possibili rischi legati al mondo del digitale riguardano:

- Proprietà (es. furto dei dati della carta di credito)
- Privacy (es. diffusione di dati strettamente personali)
- Libertà (es. censura)

Le tipologie di attacco più comuni:

- **Phishing**: truffe effettuate attraverso la rete. Normalmente consistono nel chiedere dati o denaro.
- **Malware**: qualsiasi strumento informatico progettato per danneggiare un sistema e utilizzato senza il consenso del proprietario.

Le tipologie di **Malware** più comuni:

- Adware: software che intasano il computer con annunci pubblicitari e modificano le impostazioni del browser per mostrare popup e reindirizzare gli utenti su pagine non desiderate.
- Spyware: raccolgono informazioni rispetto all'attività dell'utente senza il suo consenso e le ritrasmettono a chi sta facendo l'attacco.
- Keylogger: sono in grado di intercettare e catturare ciò che viene digitato sulla tastiera senza che l'utente se ne accorga.
- Ramsonware: questo tipo di malware cripta i file del computer e lo blocca. Sono pensati per chiedere un riscatto al proprietario in cambio dell'accesso al proprio dispositivo.
- Cryptomining: vengono installati nel computer e ne sfruttano le capacità di calcolo e l'energia per generare (minare) criptovalute.

AUTODIFESA DIGITALE

Ci sono alcune buone pratiche fondamentali che vanno accompagnate da un ragionamento (processo) rispetto a ciò che si sta facendo.

Le buone pratiche sono un inizio ma spesso da sole non bastano.

Ricordiamo sempre:

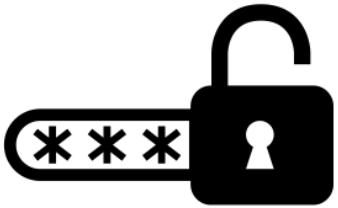
- Non ci sono soluzioni facili (non basta scaricare un'app)
- La fiducia deve essere motivata e spesso le relazioni si modificano nel tempo
- Occhi aperti e spirito critico

Domande

Buone pratiche

Password

Le password sono la **prima barriera di accesso ai dati**, le usiamo per leggere la posta, per entrare nel computer e nei mille servizi digitali a cui accediamo.



Gli errori più comuni sono:

- utilizzo di password troppo facili o banali (es. 123, password, …)
- utilizzo di elementi facili da conoscere e per noi da ricordare (es. nomi e date importanti)
- utilizzo della stessa password per servizi differenti

Buone pratiche:

La soluzione più semplice consiste nell'utilizzare un **Password Manager**, in modo tale da dover utilizzare e **ricordare solo una password** (possibilmente difficile e randomica).

Se ci sembra troppo difficile e complesso possiamo provare a:

- Cambiare spesso le password e non condividerle
- Utilizzare come password delle combinazioni di parole e lettere non semplici da individuare

WEB

Il Web è un’immensa risorsa però non è assolutamente privo di rischi, perciò quando si naviga su Internet bisogna essere consapevoli dei potenziali pericoli che potremmo dover affrontare.

Alcune operazioni preliminari:

- Router: cambiate la password di default dell’interfaccia di gestione
- Dal telefono, disabilitare il wifi (ed anche il bluetooth) quando non lo usate.

Buone pratiche:

- Controlla sempre la barra di navigazione soprattutto quando devi inserire dati della carta di credito o credenziali (https? il nome del sito è corretto?)
- Attenzione ai link sospetti, controllare prima di cliccare
- Meglio non salvare le password sul browser
- Attenzione agli allegati delle mail

Se vogliamo evitare che altre persone possano spiare la nostra navigazione (ad esempio quando utilizziamo computer in condivisione) ricordiamoci di utilizzare la **navigazione in incognito**.

- non salva la cronologia
- i file scaricati non vengono mostrati nei download
- non salva i cookie (non rimane loggato in sessioni successive)

Domande

Social Media

Quando utilizziamo i Social Media dobbiamo tenere ben presente che, oltre a fare attenzione rispetto adi altri utenti dobbiamo prestare attenzione anche alla piattaforma che li ospita.

Se non paghi il prodotto, il prodotto sei tu

Le piattaforme social offrono i loro servizi in cambio di una profilazione continua. Se vogliamo renderci conto dei dati che stiamo donando al singolo social possiamo farci un giro nei contratti/policy che abbiamo sottoscritto al momento dell'iscrizione

Ciò che metti in rete è molto facile da inserire ma estremamente difficile da togliere

Non dobbiamo mai dimenticarci che, indipendentemente da come abbiamo configurato i nostri social, tutto quello che condividiamo potrebbe potenzialmente diventare pubblico o essere usato per fini differenti rispetto a quelli che abbiamo scelto.

Il nostro livello di rischio digitale sui Social media:

- Prima di postare o far girare una notizia fai delle verifiche?
- Riesci a fare una lista di tutti i tuoi profili social, personali e di gruppo?
- Conosci personalmente i tuoi amici sui social?
- Presti attenzione nell'accettare nuovi amici sui social, in particolare quando non li conosci?
- Hai impostato una email di recupero per i tuoi account?

Se alla gran parte delle domande la tua risposta è "no" forse è il caso di pensare a come correggere il proprio rapporto con i Social.

Alcune impostazioni preliminari:

- Limitare l’accesso ai propri profili e la visibilità delle informazioni ai soli contatti
- Account personale, evitiamo la condivisione dell’account o la condivisione dei dati di accesso
- Scegliere molto accuratamente la password di accesso e impostare una mail di recupero

Buone pratiche:

- Evitare di condividere la nostra posizione in tempo reale
- Fare attenzione nell'accettare "nuove amicizie" soprattutto quando non conosciamo realmente le persone e provvedere alla pulizia dei contatti nel caso fosse necessario
- Verificare sempre le notizie o in generale i post prima di condividerli, in modo da evitare di promuovere fake news
- Prestare attenzione ai dati personali che si vuole condividere (informazioni o media)
- Evitare di "taggare" altri account senza il loro consenso, e impostare il controllo dei tag sul proprio profilo
- In generale: evitare di prestare troppa fiducia nello strumento

Domande

Smartphone

Lo smartphone è ormai nelle tasche di tutti, ma non sempre ci rendiamo conto fino in fondo dello strumento e dei rischi che comporta.

La nostra vita in tasca

Spesso all’interno del nostro telefono sono presenti tutti o tanti dei nostri dati più sensibili. Cerchiamo di capire come rendere un po più sicuro l’utilizzo dello smartphone.

Alcune impostazioni preliminari:

- Impostare una password sicura e ricordatevi di cambiarla ogni tanto o se l’avete condivisa con qualcuno
- Configurare da soli il proprio smartphone o essere presenti se viene configurato da qualcun altro
- Impostare la possibilità di cancellare i dati da remoto in caso di furto
- Se decidiamo di regalare a qualcuno il nostro vecchio telefono ricordiamoci di effettuare il ripristino ai dati di fabbrica (reset)

Buone pratiche:

- Evitare di condividere o prestare lo smartphone
- Evitare di tenere accesi wifi, bluetooth e posizione quando non li stiamo utilizzando (anche la batteria ringrazia!)
- Installare solo le app necessarie e fare attenzione nella scelta delle stesse
- Fare attenzione ai permessi richiesti dalle app che installiamo

Domande

Instant messaging

Con Instant messaging si indica una comunicazione privata e istantanea. Entrambi gli aggettivi (privato e istantaneo) possono celare delle ambiguità a cui dobbiamo stare attenti.

Quando la comodità può diventare scomoda

Il privato può facilmente diventare pubblico se la nostra fiducia non è giustamente riposta.
L'istantaneità può essere un'arma a doppio taglio e può facilmente diventare uno strumento di controllo.

Alcune impostazioni preliminari:

- Utilizziamo le giuste app a seconda dello scopo e, se necessario, impostiamo una password per l'accesso
- Valutiamo se eliminare le "spunte" e in generale modifichiamo le impostazioni sulla privacy
- Eliminiamo la geolocalizzazione fra le impostazioni

Buone pratiche:

- Utilizzare Signal e impostare i messaggi a scomparsa per la condivisione di materiale sensibile (però ricorda che Signal è molto meno sicuro se viene utiizzato sul PC)
- Elimina le spunte anche in un secondo momento se ti rendi conto che sono diventate uno strumento di controllo da parte di qualcuno
- Attenzione alla gestione e utilizzo dei gruppi, silenzia le notifiche e/o abbandona i gruppi che non ti servono
- Ricordiamo che esistono anche altri strumenti e che non sempre la messaggistica istantanea è quello corretto

Domande

Molestie online

Nel mondo del digitale può risultare più difficile riconoscere spazi non sicuri ed inoltre l'anonimato può rivelarsi un'arma a doppio taglio.

"Don't feed the troll" e non solo

Ricordiamoci inoltre che il mondo digitale ha delle ripercussioni anche sul mondo reale, perciò cerchiamo di prevenire o quantomeno limitare ciò che può accadere.

I rischi più comuni:

- Trolling - Si parla di trolling quando delle persone che non fanno parte del gruppo di riferimento entrano a gamba tesa in un discorso e tentano di creare argomentazioni controverse e conflittuali per attirare l'attenzione verso di se.
- Stalking - insieme di comportamenti persecutori ripetuti e intrusivi, come minacce, pedinamenti, molestie, telefonate o attenzioni indesiderate.
- Cyber bullismo - manifestazione attraverso la rete di azioni violente e intimidatorie esercitate da un singolo, o un gruppo, su qualcuno.
- "Revenge" porn - condivisione non consensuale di media a sfondo sessuale, parlare di "revenge" (vendetta) non è corretto in quanto può creare una parziale legittimazione.

Buone pratiche:

- Evitiamo di alimentare polemiche sterili soprattutto quando non conosciamo direttamente il nostro interlocutore: “Don’t feed the troll”.
- Ricordiamoci sempre che la fiducia può modificarsi nel tempo.
- Cerchiamo di essere sempre chiari nelle nostre comunicazioni, se qualcosa non ci piace o ci fa stare male diciamolo chiaramente. Se riceviamo un “no” accettiamolo senza insistere e, dall’altra parte, impariamo a rispettare la sensibilità degli altri.
- Il “Ghosting” può essere uno strumento utile se l’altra persona insiste nel cercarci anche dopo il nostro rifiuto alla comunicazione.

Domande

Terminologia

Hacker / Cracker

Per hacker si intende una persona curiosa e “smanettona” che ha la tendenza a riparare o creare, mentre nel cracker la tendenza è quella di distruggere o aggirare. Entrambe le figure possono svolgere la loro attività in ambiti legali o no e in modalità “etica” o no. Normalmente questi termini vengono utilizzati in ambito informatico ma sono utilizzabili anche per altre discipline.

TOR

Sistema (ma anche browser) che permette un alto grado di riservatezza, in quanto il collegamento a Internet passa attraverso diversi “nodi”, il che rende molto più difficile risalire a chi lo sta usando. Tutti i passaggi sono criptati, perciò è difficile capire cosa sta transitando sulla Rete.
Utilizzare “Tor” rende la navigazione più lenta e alcuni siti web potrebbero impedire l’uso di alcune funzioni o non essere visualizzabili.

Terminologia: Malware

Virus

Programmi che possono infettare altri file effettuando copie di loro stessi senza farsi rilevare.

Worm

Simili ai virus, si moltiplicano per infettare i computer e danneggiare dati e file, a differenza del virus non ha bisogno di interazione umana per diffondersi.

Trojan

Come il celebre cavallo inventato da Ulisse, si installano nel computer per dare accesso all'hacker, che prenderà il controllo del computer. Sono tra i più pericolosi.

Exploit

Programmi che approfittano dei punti deboli (vulnerabilità) del software o dell'hardware

Domande