50 consigli per la sicurezza digitale

Quando si parla di tecnologia ci si concentra spesso solo sulla modalità di utilizzo di computer, tablet o smartphone. La maggior complessità del mondo digitale e la tendenza naturale ad ignorare i rischi, spesso ci impediscono di vedere e capire le nuove minacce.
Questo documento vuole dare alcuni consigli di comportamento per stare alla larga dai pericoli inattesi.

Impariamo a conoscere il mondo digitale

- Anche su internet cerchiamo di avere un **comportamento prudente** e una **diffidenza ragionevole** come nel mondo reale.
- Evitiamo di fare nel **mondo digitale** quello che non faremmo mai nel **mondo reale.**
- Attenzione ai **contatti** su internet: siamo sempre di fronte ad un **estraneo** che non conosciamo, anche se si mostra come un amico.
- Rifiutiamo le richieste di amicizia inviate da **sconosciuti**. Chiediamoci perché dovrebbero contattarci.
  Per saperne di più → *https://bit.ly/3l4K2Ec*
- Evitiamo di incontrare nel **mondo reale** persone che abbiamo conosciuto **solo online.**
- Valutiamo quali sono le nostre **informazioni più importanti da proteggere** e quali **non devono essere rese pubbliche**.
- Proteggiamo la nostra **privacy** perché ogni attività che facciamo su Internet resta **memorizzata per sempre**.
  Per saperne di più → *http://bit.ly/2Dexsg9*
- Prestiamo attenzione nel pubblicare **dati e informazioni** su Internet e sui social network. Come potrebbero **essere usate dagli altri**?
  Per saperne di più → *http://bit.ly/1QwQw5M*
- Attenzione alla perdita dei dispositivi mobili (portatili, smartphone, tablet, ecc.) non per il loro valore, ma per i **dati contenuti**.
- Chi ci attacca è sempre in vantaggio perché si concentra su **un solo obiettivo** mentre noi dobbiamo difenderci da **tutti i possibili rischi.**
- Siamo **prudenti** su tutto quanto troviamo su Internet: messaggi, informazioni e persone. Dietro a situazioni apparentemente interessanti **possono nascondersi molti tipi di truffe**.
  Per saperne di più → *http://bit.ly/3zVSxrw*
- Attenzione alle comunicazioni e ai messaggi che provengono dai **social network** perché potrebbero anche loro nascondere **degli imbrogli.**
  Per saperne di più → *http://bit.ly/2nFHGPB*
- Verifichiamo l'autenticità e l'autorevolezza della fonte per evitare di essere imbrogliati dalle fake news.
  Per saperne di più → *https://bit.ly/2VxVPSY*

Cerchiamo di prendere le decisioni giuste

- Prestiamo attenzione ai messaggi di posta ricevuti da sconosciuti: spesso nasconde messaggi di **phishing** che ci indirizzano verso **siti falsificati per operare delle truffe**.
  Per saperne di più → *http://bit.ly/3E0vBdj*
- Nel caso di messaggi di posta ricevuti da sconosciuti **non bisogna mai cliccare sui link o aprire eventuali allegati**.
- Diffidiamo delle offerte allettanti così come degli annunci di situazioni allarmanti che ci spingono ad agire di impulso. Prima di fare qualsiasi cosa è **meglio riflettere ed informarsi**.
  Per saperne di più → *http://bit.ly/3zVSxrw*
- Cerchiamo di essere rispettosi della nostra persona e teniamo sotto controllo la **nostra immagine online**. Non pubblichiamo foto di cui in futuro potremmo pentirci.
- Non pubblichiamo foto nostre o di altri che contengono i dati di **localizzazione geografica** per non fornire informazioni ai malintenzionati.
  Per saperne di più → *https://bit.ly/3hnaJ6i*
- Non pubblichiamo **foto dei nostri figli** per evitare che vengano identificati da malintenzionati.
  Per saperne di più → *https://bit.ly/2XfdXBV*
- Su Internet rispettiamo gli altri e la loro **vita privata** ed evitiamo di creare **situazioni spiacevoli,** visibili **da numerose persone** e che **durano nel tempo**.
  Per saperne di più → *http://bit.ly/2nHTUGy*
- **Denunciamo chi ci molesta** – memorizziamo le conversazioni, blocchiamo i contatti e non rispondiamo ai messaggi.
- Navighiamo e scarichiamo files solo da **siti riconosciuti e affidabili.**
  Per saperne di più → *http://bit.ly/2oT4dsf*
- In Svizzera è possibile scaricare musica gratuitamente ma **non è legale ridistribuirla**.
  Per saperne di più → *http://bit.ly/3w7ezFr*
- In caso di dubbio su situazioni insolite **possiamo utilizzare i motori di ricerca** (Google, DuckDuckGo, Bing, ecc.) per verificare se siamo di fronte a possibili truffe o imbrogli.
- Cerchiamo di **restare informati** e **condividiamo con gli altri** le conoscenze e le informazioni su come restare sicuri e protetti nella rete.

Proteggiamo le nostre informazioni e la nostra identità digitale

- Per proteggere le nostre informazioni dobbiamo utilizzare una buona **password** che **non dobbiamo comunicare a nessuno** o **scriverla/ memorizzarla in modo non sicuro**.
  Per saperne di più → https://bit.ly/3tvJ4Vw
- La password deve avere una lunghezza di a**lmeno 12 caratteri**, e includere numeri, simboli, lettere maiuscole e minuscole
  Aggiungendo una virgola (,) alla password riuscite a creare problemi a chi ruba i database di password.
- La password non deve contenere **informazioni personali** o altri dati facilmente intuibili.
- I **sistemi biometrici** (impronte digitali, immagine del viso, ecc.) sono molto pratici da usare sui **sistemi portatili** ma non riescono a sostituire le **password dei siti internet**.
  Per saperne di più → https://bit.ly/36tx8HP
- Una buona password dovrebbe essere tenuta a mente e per questo deve essere **facile da ricordare** ma **difficile da indovinare**.
  Per saperne di più → https://bit.ly/3ogPRQc
- La password va cambiata solo quando si ha il sospetto o la certezza che sia stata scoperta da altri.
  Per saperne di più → https://bit.ly/2QMIcdD
- Nel caso di accesso a dati sensibili è importante utilizzare l'autenticazione a due fattori con un secondo elemento (qualcosa che si conosce o si possiede o una caratteristica personale).
- *Per saperne di più →* https://bit.ly/2YKwZ3x
- È indispensabile usare password differenti per informazioni/siti e apparecchi differenti.
  Per saperne di più → https://bit.ly/1PwkRqT
- Per poter facilitare l'uso di diverse password è utile utilizzre un programma di gestione delle password (**password manager**).
  Per saperne di più → https://bit.ly/2KOVd2J
- È possibile verificare se le **nostre password** sono state **rubate** su un sito che memorizza tutti furti di password.
  Per saperne di più → https://bit.ly/2Q8gOZC
- È possibile verificare la **robustezza** di una **password** su un sito che permette di simulare un attacco.
  Per saperne di più → https://bit.ly/2OYYE9d

Restiamo sicuri e protetti

- È importante **bloccare lo schermo** del computer con una **password** per evitare che estranei vedano le nostre informazioni.
- È importante bloccare lo schermo del nostro **tablet/smartphone** utilizzando il **PIN, l'impronta digitale o l'immagine del viso** per proteggere le nostre informazioni in caso di furto/smarrimento.
  Per saperne di più → https://bit.ly/3jZh3lU
- Prestiamo attenzione a non fornire il nostro indirizzo di posta elettronica a sconosciuti che potrebbero usarlo per inviarci dello **spam**.
  Per saperne di più → https://bit.ly/2YJP1D0
- Assicuriamoci di avere istallato un **antivirus aggiornato** (sono validi anche quelli gratuiti) e un **personal firewall**.
  Per saperne di più → https://bit.ly/2OKmHHM
- Manteniamo **aggiornati** il software di base e le applicazioni del nostro computer e del nostro tablet/smartphone. Abilitiamo gli **aggiornamenti automatici.**
  Per saperne di più → https://bit.ly/2QNEj8y
- Facciamo regolarmente una **copia dei dati importanti** del nostro computer su un disco esterno o una chiavetta USB (backup).
  Per saperne di più → https://bit.ly/1MQp20u
- Salviamo regolarmente i **dati** del nostro **smartphone/tablet** sul nostro **computer** o sul **cloud.**
- Assicuriamoci di **cancellare tutte le nostre informazioni** in caso di smaltimento degli apparecchi.
  Per saperne di più → https://bit.ly/2FINTAO
- Per inviare **informazioni riservate** per posta elettronica o sistemi di messaggistica è indispensabile utilizzare la **crittografia**.
  Per saperne di più → https://bit.ly/2KOPvhm

Link utili

- Rassegna stampa sulla sicurezza informatica
  https://twitter.com/silvanomarioni
- Glossario dei termini di sicurezza
  http://bit.ly/1qSPPif
- Centro nazionale per la cibersicurezza
  www.ncsc.admin.ch/ncsc/it/home.html
- eBanking ma sicuro!
  https://www.ebas.ch/it/