Consigli e suggerimenti

Adottate le buone prassi di sicurezza online con questi consigli e suggerimenti. La presente sezione è stata allestita in collaborazione con Get Safe Online (Regno Unito) e con il Dipartimento di sicurezza nazionale statunitense.

- Proteggete il vostro personal computer (PC) e i vostri dispositivi portatili
- Proteggete la vostra identità e i vostri dati personali
- Proteggete le informazioni aziendali al di fuori della vostra organizzazione
- Connettetevi con le dovute precauzioni
- Conoscete il web

Proteggete il vostro personal computer (PC) e i vostri dispositivi portatili

PC

- Usate un firewall: i firewall proteggono la vostra rete da virus e hacker
- Installate un software antivirus: i software antivirus impediscono ai virus di colpire il vostro computer
- Scaricate gli ultimi aggiornamenti di sicurezza: mantenete le vostre applicazioni e il vostro sistema operativo funzionanti e aggiornati
- Bloccate gli spyware: impedite agli estranei di penetrare nel vostro computer, evitando e-mail e allegati sospetti
- Effettuate regolari backup: proteggete i dati dalla distruzione

Laptop

- Spegnete le connessioni wireless quando non sono necessarie o non le utilizzate
- Connettete regolarmente il vostro laptop a una rete sicura per scaricare gli aggiornamenti di sicurezza
- Effettuate il backup dei dati salvati nel vostro laptop
- Non lasciate il laptop incustodito

Driver USB

- Usate un driver USB criptato
- Impostate la modalità di sola lettura del driver flash USB usando l'interruttore fisico per evitare la trasmissione di virus: alcuni driver flash USB includono un interruttore fisico per impostare il driver in modalità di sola lettura ed evitare che il computer host scriva o modifichi i dati sul driver

- Effettuate una scansione del driver flash USB dopo aver copiato file da una sorgente non sicura e/o non autorizzata per evitare la trasmissione di virus
- Prima di collegare il driver USB al computer di qualcun altro, cancellate tutti i file che non sono rilevanti ai fini di tale azione
- Eseguite il backup dei dati presenti nel vostro driver USB per recuperarli in caso di distruzione
- Attaccate i driver USB a portachiavi / cordini per evitare che vadano persi: a causa delle loro piccole dimensioni, questi dispositivi possono essere facilmente smarriti o rubati. Inoltre, la più elevata capacità di memoria accresce la quantità potenziale di dati a rischio di accesso non autorizzato. I driver flash USB sono generalmente riposti in borse, zaini, custodie per laptop, giacche e tasche di pantaloni o lasciati su postazioni di lavoro sguarnite. Il numero di incidenti è recentemente cresciuto, in quanto i driver USB vengono smarriti, mal riposti, presi in prestito senza permesso o rubati.

Telefoni cellulari e palmari

I palmari come i dispositivi Windows Mobile, Palm, iPhone, Android e Blackberry sono dotati di connessioni a Internet e sono in grado di memorizzare un'enorme quantità di dati. La loro estrema portabilità fa sì che debbano essere trattati con la massima cura.

- Spegnete le connessioni wireless (Bluetooth e WLAN) quando non le utilizzate. La tecnologia Bluetooth permette ai dispositivi elettronici di comunicare gli uni con gli altri utilizzando un collegamento radio a corto raggio.
- Non lasciate il telefono cellulare e il palmare incustoditi. Potreste rischiare di perdere i dati.
- Utilizzate la funzione password per prevenire l'hacking remoto nel vostro smartphone.

Proteggete la vostra identità e i vostri dati personali

- **Usate una password sicura**: la vostra password è l'equivalente della serratura e della chiave della vostra casa su Internet. Le password sono un'importante forma di difesa e adottare buone prassi a questo riguardo vi aiuterà a tenere più al sicuro la vostra identità e i vostri dati personali sensibili. La password del vostro computer è la chiave per accedere a tutti i dati – sia aziendali sia personali – che avete salvato nel vostro computer e nei vostri account online. Utilizzate una password sicura per proteggere i vostri dati: usate una serie complessa di caratteri, combinando lettere (maiuscole e minuscole), numeri e simboli. Quanto più vari saranno i caratteri presenti nella vostra password, tanto più difficile sarà risalirvi. Non utilizzate informazioni personali – nome, nomi dei figli, date di nascita ecc. – che qualcuno possa già conoscere o ottenere facilmente e cercate di evitare le parole di uso comune: alcuni hacker utilizzano programmi che provano ogni singola parola presente nel dizionario.
- **Cambiate regolarmente la vostra password**: se pensate che il vostro sistema sia stato compromesso, cambiate immediatamente le password.

- **Tenete segreta la vostra password**: la vostra password è unica e non deve essere condivisa con nessuno. Ove possibile, cercate di ricordare le password a memoria. Usate una strategia per memorizzarle. Se le scrivete, fate attenzione a dove le conservate. Non lasciate queste registrazioni delle vostre password in luoghi in cui non lascereste le informazioni da esse protette.
- **A ogni account la sua password**: usate password differenti per ogni account online a cui avete accesso (o almeno una serie di password diverse). Se usate le stesse password per più account, un intruso che dovesse riuscire ad accedere a un account avrà accesso anche a tutti gli altri vostri account.
- **Mettete al sicuro i vostri account**: molti account provider offrono mezzi supplementari per verificare la vostra identità prima che possiate operare sul sito in questione.
- **Esercitate il controllo sulla vostra presenza online**: se disponibili, impostate le funzioni di privacy e di sicurezza dei siti web sul livello di condivisione delle informazioni che desiderate. È preferibile limitare gli utenti con i quali condividete informazioni.
- **Utilizzate con cautela i siti dei social network**: tenete presente che i siti dei social network possono riunire molti dei rischi associati alla vostra presenza online; bullismo online, divulgazione di informazioni private, cyber-stalking, accesso a contenuti non adatti all'età e, nei casi più estremi, adescamento e pedofilia online.

Proteggete le informazioni aziendali al di fuori della vostra organizzazione

- **Assicuratevi di tenere al sicuro i vostri dati sensibili**: quando vi trovate al di fuori della vostra organizzazione, accertatevi di tenere al sicuro in ogni momento i vostri dispositivi e dati sensibili per evitare che siano rubati o smarriti. Trattate i dati con cura soprattutto quando vi trovate in luoghi pubblici.
- **Tenete riservate le informazioni aziendali**: siate consapevoli che qualcuno potrebbe ascoltare la vostra conversazione. Non mettete a disposizione di chiunque le informazioni riservate della vostra organizzazione.
- **Siate consapevoli dello shoulder surfing**: quando siete in viaggio o lavorate da una postazione remota, proteggetevi dallo shoulder surfing.
- **Usate la webmail con attenzione**: usare un browser Internet per leggere la vostra posta richiede la stessa attenzione che prestereste con un sistema di desktop mail e comporta alcuni rischi specifici per la sicurezza.

Connettetevi con le dovute precauzioni

- **Spegnete le connessioni wireless quando non sono necessarie o non le utilizzate**
- **Usate gli hotspot Wi-Fi con parsimonia**: quando utilizzate gli hotspot Wi-Fi, riducete il tipo di attività che svolgete e regolate le impostazioni di sicurezza del vostro dispositivo in modo da limitare il numero di utenti che possono accedervi.
- **Proteggete i vostri soldi**: quando effettuate operazioni bancarie e fate acquisti online, assicuratevi che i siti siano security-enabled. Cercate indirizzi web che inizino con https:// o

shttp://, che significa che il sito adotta misure supplementari per tutelare i vostri dati. I siti http:// non sono sicuri.

- **Bloccate le e-mail indesiderate**: lo spam è una minaccia per la sicurezza. Non aprite e-mail e allegati inviati da sconosciuti.
- **In caso di dubbio, cestinateli**: se i link presenti in e-mail, tweet, post e pubblicità online appaiono sospetti, anche se ne conoscete la provenienza, è meglio cancellarli o, se del caso, contrassegnarli come junk mail.
- **Inoltrate le e-mail solo se appropriato:** valutate se cancellare i precedenti passaggi del messaggio prima di effettuare l'inoltro.
- **Fate attenzione quando navigate in Internet.**
- **Non scaricate documenti e materiale da fonti non sicure.**
- **Fate attenzione quando usate computer pubblici:** connettetevi a un computer pubblico soltanto se avete una connessione criptata (indicata dal lucchetto nella parte in basso a destra della finestra del vostro browser e dalle lettere https:// all'inizio dell'indirizzo del sito web).
- **Utilizzate i servizi webmail di società conosciute e fidate.**

Conoscete il web

- **Tenetevi aggiornati:** tenetevi al passo con i nuovi sistemi per navigare sicuri online: verificate le ultime informazioni pubblicate su siti sicuri, condividetele con la famiglia, gli amici e i colleghi e incoraggiateli a conoscere il web. Rendete sicuro il vostro browser.
- **Pensate prima di agire**: state attenti alle comunicazioni che vi suggeriscono di agire immediatamente, che offrono qualcosa che sembra troppo bello per essere vero o che richiedono informazioni personali.
- **Eseguite il backup**: proteggete il vostro lavoro, la vostra musica, le vostre foto e altre informazioni digitali, facendone una copia elettronica e salvandola in modo sicuro.