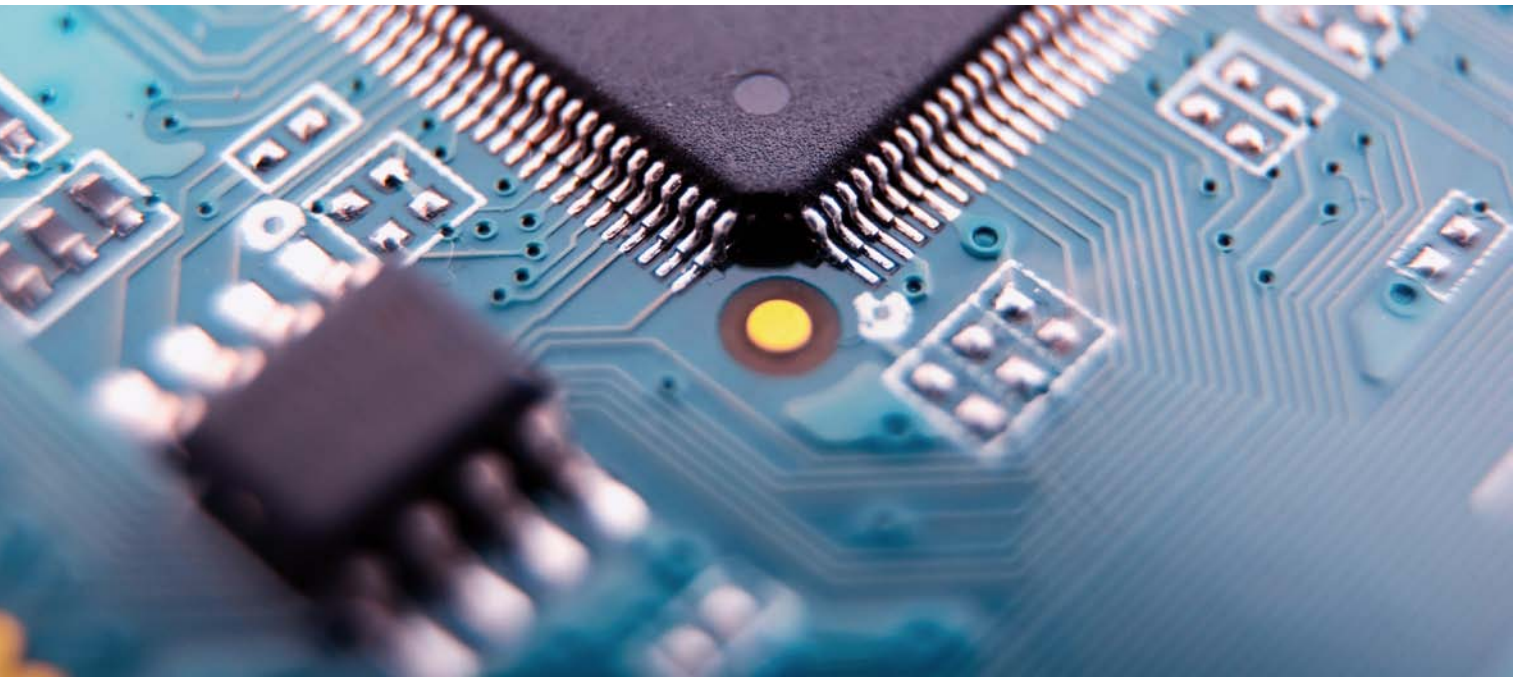
CREDIT SUISSE

Guida alla sicurezza informatica

Sommario

Sicurezza informatica



Per noi di Credit Suisse, la sicurezza dei vostri dati è sempre in primo piano. Ci impegniamo per tutelare i nostri sistemi, software, reti e altri asset tecnologici, proteggendoli dagli attacchi di utenti non autorizzati, che tentano di sottrarre o distruggere informazioni riservate, causare disservizi o altri danni.

Abbiamo collaboratori in tutto il mondo che si dedicano alla tutela della sicurezza informatica, ad esempio collaborando con enti regolatori, forze dell'ordine e altri enti, al fine di consolidare le nostre difese e potenziare la resilienza di fronte alle minacce.

In una realtà dominata da social network, transazioni online, cloud computing e processi automatizzati, la tecnologia è in rapida e continua evoluzione. Ma di pari passo con il progresso tecnologico dilaga il fenomeno dei **crimini informatici**, che si traducono costantemente in nuovi tipi di attacchi, strumenti e tecniche per fare breccia in ambienti sempre più sofisticati e protetti, causando gravi danni, talvolta senza lasciare traccia.

Molto probabilmente Internet è parte integrante di tutto ciò che fate; di conseguenza, i crimini informatici rappresentano una grave e crescente minaccia. Ecco perché è **essenziale** che la prevenzione delle frodi diventi per tutti un aspetto imprescindibile delle attività quotidiane.

Scopo del presente libretto è fornirvi suggerimenti utili per proteggere voi stessi, i vostri beni e i vostri dati personali dai criminali online.

Lista di controllo per la sicurezza informatica

Alcuni suggerimenti per proteggere computer e denaro dagli attacchi dei criminali online

1.
Installate e tenete costantemente aggiornati programmi di protezione in grado di riconoscere le minacce incombenti. Installate sul vostro computer software antivirus che offrano protezione contro i malware (software malevoli) in grado di sottrarre informazioni come numeri di conto e password, e utilizzate un firewall per prevenire gli accessi non autorizzati.

2.
Siate cauti nella scelta dei luoghi e delle modalità di accesso a Internet per le vostre operazioni bancarie o altre comunicazioni che prevedano lo scambio di dati personali sensibili. Le reti Wi-Fi pubbliche e i computer installati in luoghi come biblioteche o centri business- possono essere rischiosi se non provvisti di software di protezione aggiornati.

3.
Acquisite familiarità con le funzioni di sicurezza standard di Internet. Installate sul vostro computer software antivirus che offrano protezione contro i malware (software malevoli) in grado di sottrarre informazioni come numeri di conto e password e utilizzate un firewall per prevenire gli accessi non autorizzati.

4.
Ignorate le e-mail non richieste che vi invitano ad aprire un allegato o cliccare su un link, a meno che non siate assolutamente certi del mittente e del motivo dell'invio. I criminali informatici creano abilmente e-mail fasulle che sembrano plausibili, ma possono installare software malevole. Se ricevete un'e-mail inaspettata con la richiesta di aprire un allegato o un file, potete ignorarla oppure accertarvi che la presunta fonte vi abbia realmente inviato il messaggio, contattandola telefonicamente o tramite un indirizzo di posta elettronica ufficiale.

5.
Siate prudenti se qualcuno vi contatta inaspettatamente online, chiedendovi i vostri dati personali. La cosa migliore è ignorare le richieste di informazioni inaspettate, per quanto possano apparire plausibili, soprattutto se l'oggetto del messaggio sono informazioni come numeri di assicurazione e di conti bancari oppure password.

6.
Scegliete la procedura più sicura possibile per accedere ai vostri conti finanziari. Create password efficaci, difficili da scoprire, cambiatele regolarmente e cercate di evitare l'uso della stessa password o dello stesso PIN (numero di identificazione personale) per più conti.

7.
Prestate attenzione quando accedete ai siti di social networking. I criminali setacciano questi siti alla ricerca di informazioni come il luogo di nascita, il cognome da nubile di vostra madre o il nome dell'animale domestico, sperando di trovare dati utili per indovinare o resettare le password degli account online.

8.
Fate attenzione quando utilizzate smartphone e tablet. Non lasciate il vostro dispositivo mobile incustodito e proteggetelo, mediante password o in altro modo, da accessi indebiti in caso di furto o smarrimento.

Sicurezza informatica personale a colpo d'occhio

Proteggete il vostro computer.

Installate appositi software contro i malware, o software malevoli, in grado di accedere al sistema senza il vostro consenso per appropriarsi di password o numeri di conto. Inoltre, utilizzate un firewall per prevenire l'accesso non autorizzato. Esistono sul mercato diverse opzioni di protezione; accertatevi in ogni caso che le impostazioni prevedano aggiornamenti automatici.

Utilizzate il metodo più sicuro per accedere agli account finanziari.

Utilizzate l'autenticazione più sicura possibile, soprattutto per le transazioni ad alto rischio. Scegliete password difficili da scoprire e non rivelatele a nessuno. Create ID utenti e password efficaci per i vostri computer, dispositivi mobili e account online utilizzando combinazioni di lettere maiuscole e minuscole, numeri e simboli difficili da indovinare e non dimenticate di cambiarle regolarmente. Per quanto comodo possa essere utilizzare la stessa password o lo stesso PIN per diversi account, così facendo offrite a un criminale la possibilità di accedere a diversi vostri sistemi.

Acquisite familiarità con le funzioni di protezione di Internet.

Se l'indirizzo web inizia con "https://.", esistono maggiori garanzie sull'autenticità del sito e sulla cifratura (codifica) dei vostri dati in fase di trasmissione. Inoltre assicuratevi di uscire dagli account finanziari una volta completate le transazioni o quando vi allontanate dal computer. Per informazioni su altre procedure di sicurezza, consultate le istruzioni d'uso del vostro browser di rete.

Fate attenzione alle e-mail inaspettate

Fate attenzione alle e-mail inaspettate che invitano a cliccare su un link, scaricare un allegato o fornire informazioni sul vostro account. Per i criminali informatici è facile copiare il logo di un'azienda o un'organizzazione nota in un'e-mail di phishing. Rispondendo a una semplice richiesta, potreste installare il malware. La strategia migliore è ignorare le richieste inaspettate, per quanto possano apparire plausibili o allettanti.

Scegliete con cura i luoghi e le modalità per collegarvi a Internet.

Per svolgere operazioni bancarie o altre attività che prevedano lo scambio di dati personali dal laptop e esclusivamente connessioni sicure, note e affidabili. Un computer pubblico, ad esempio presso il centro business di un hotel o una biblioteca, e le reti Wi-Fi gratuite non rispondono sempre a questi requisiti. Per un criminale informatico può essere relativamente facile intercettare il traffico Internet che passa attraverso queste postazioni.

Prestate attenzione quando accedete ai siti di social networking.

I criminali informatici ricorrono ai siti di social networkingper raccogliere dati personali, ad esempio il luogo o la data di nascita, il nome di un animale domestico, il cognome da nubile di vostra madre e altre informazioni utili per indovinare o resettare le password. Non condividete i vostri profili o l'accesso alle vostre informazioni con persone che non conoscete e di cui non vi fidate. I criminali informatici tentano di diventare vostri "amici" per convincervi a inviare denaro o divulgare informazioni personali.

Prendete le opportune precauzioni per il tablet o lo smartphone.

Per il sistema operativo del vostro dispositivo e le "app" (applicazioni), prendete in considerazione l'opzione degli aggiornamenti automatici in modo da ridurre la vulnerabilità ai problemi di software. Non lasciate mai il vostro dispositivo mobile incustodito e utilizzate una password o un'altra funzione di protezione per limitare l'accesso al dispositivo in caso di furto o smarrimento. Accertatevi di aver abilitato la funzione "time-out" o "blocco automatico" che interviene nel caso di un periodo di inattività prolungato. Prima di scaricare qualsiasi app, fate adeguate ricerche.

Sicurezza informatica in azienda a colpo d'occhio

Proteggete i computer e le reti.

Installate software di sicurezza e programmi antivirus in grado di offrire protezione contro i malware o software malevoli che, senza il consenso del titolare, possono accedere al sistema di un computer per diversi scopi, tra cui il furto di dati. Inoltre, utilizzate un firewall per prevenire accessi non autorizzati. Le opzioni di protezione sono diverse, quindi individuate quella più adeguata alle dimensioni e alla complessità della vostra attività. Quando opportuno, aggiornate il software in modo che sia sempre efficace. Ad esempio, configurate il programma antivirus in modo che esegua una scansione dopo ogni aggiornamento. Se utilizzate una rete wireless (Wi-Fi), accertatevi che sia sicura e cifrata. Proteggete l'accesso al router con password ben strutturate.

Richiedete autenticazioni efficaci.

Accertatevi che i collaboratori e gli altri utenti che si collegano alla vostra rete utilizzino ID utenti e password idonei per computer, dispositivi mobili e account online, ricorrendo a combinazioni di lettere maiuscole e minuscole, numeri e simboli difficili da indovinare, e che vengano regolarmente cambiate. Prendete in considerazione l'implementazione di autenticazioni a più fattori che al momento dell'accesso richiedono informazioni aggiuntive oltre alla password. Accertatevi che i fornitori che gestiscono dati sensibili offrano autenticazioni di questo tipo per l'accesso a sistemi o account.

Controllate l'accesso ai dati e ai computer

Controllate l'accesso ai dati e ai computer e create un account utente per ciascun collaboratore. Adottate misure appropriate per limitare l'accesso o l'uso dei computer aziendali da parte di soggetti non autorizzati. Custodite sotto chiave i laptop quando non sono in uso per non incorrere in furti o smarrimenti. Chiedete a ogni collaboratore di utilizzare un account utente separato e vietate la condivisione degli account. Fornite l'accesso solo ai sistemi di dati di cui i collaboratori necessitano per svolgere le loro mansioni e non consentite l'installazione di software senza previa autorizzazione. Inoltre assicuratevi che i diritti di amministrazione siano concessi solo ai collaboratori che ne hanno effettivamente bisogno, come il personale del reparto IT e le persone chiave, e riesaminate periodicamente la loro necessità di accesso.

Assicuratevi che i collaboratori siano formati.

Stabilite norme e direttive di sicurezza per i collaboratori, come linee guida per l'uso di Internet, e definite requisiti e conseguenze in caso di violazione. Promuovete una cultura aziendale top-down che sottolinei l'importanza di un'adeguata sicurezza informatica, soprattutto in tema di gestione e protezione dei dati dei clienti e di altre informazioni critiche. Assicuratevi che tutti i collaboratori sappiano identificare e segnalare potenziali minacce per la sicurezza, e che inoltre facciano attenzione a scegliere i luoghi e le modalità per collegarsi a Internet. Per accedere alla vostra rete, collaboratori e utenti terzi devono utilizzare esclusivamente connessioni sicure e affidabili. I computer pubblici, ad esempio presso un Internet café, il centro business di un hotel o una biblioteca, non lo sono sempre. Inoltre, non è opportuno collegarsi alla rete aziendale se la connessione wireless non è sicura, come spesso accade con molte reti Wi-Fi gratuite presso "hotspot" pubblici. Per un criminale informatico può essere relativamente facile intercettare il traffico Internet che passa attraverso queste postazioni.

Informate i collaboratori sui rischi delle e-mail sospette.

I collaboratori devono prestare attenzione alle e-mail inaspettate che li invitano a cliccare su un link, aprire un allegato o fornire informazioni sull'account. Per i criminali informatici è facile copiare il logo di un'azienda o un'organizzazione nota in un'e-mail di phishing. Assecondando quella che all'apparenza risulta una semplice richiesta, i vostri collaboratori potrebbero installare malware sulla rete. La strategia migliore è ignorare le richieste inaspettate, per quanto possano apparire plausibili. I fornitori di software offrono regolarmente patch o aggiornamenti dei loro prodotti per ovviare a eventuali carenze e migliorare la funzionalità: è buona norma scaricarli e installarli appena disponibili. Una pratica soluzione è configurare il software per eseguire installazioni automatiche.

Eseguite copie di sicurezza.

Eseguite copie di sicurezza di sistemi e dati vitali. Eseguite regolarmente il backup dei dati dai computer utilizzati in azienda. Ricordate di applicare ai dati di backup le stesse misure di sicurezza adottate per i dati originali, ad esempio la cifratura. In aggiunta ai backup automatici, copiate regolarmente i dati cruciali in un dispositivo di archiviazione presso una postazione secondaria sicura.

Controllate scrupolosamente i vostri conti bancari.

Controllate scrupolosamente i vostri conti bancari e prestate attenzione a eventuali prelievi non autorizzati. Prevedete controlli aggiuntivi come chiamate di conferma prima che i trasferimenti siano autorizzati dall'istituto finanziario. Negli ultimi anni si sono moltiplicati i trasferimenti elettronici non autorizzati, effettuati da conti bancari di aziende. Una truffa comune consiste nel furto di identità: i criminali informatici utilizzano software malevoli, come logger di battitura (keystroke logger), per impossessarsi degli ID e delle password dei conti bancari online ed effettuare prelievi. Un'altra modalità (Business Email Compromise) rivolge alle aziende richieste di pagamento provenienti apparentemente da legittimi fornitori, ma che in realtà si indirizzano al conto dell'organizzazione criminale. In genere, ai sensi della normativa in materia di protezione dei consumatori, le aziende non sono tutelate contro i trasferimenti di fondi elettronici non autorizzati.

Non dimenticate tablet e smartphone.

I dispositivi mobili possono rappresentare una minaccia per la sicurezza, soprattutto se contengono informazioni riservate o sono impiegati per accedere alla rete aziendale. Se i vostri collaboratori collegano i loro dispositivi alla rete aziendale, chiedete di proteggerli con password, crittografare i dati e installare app di sicurezza per impedire l'accesso non autorizzato mentre il dispositivo è collegato a reti pubbliche. Ponete in atto e fate rispettare procedure di reporting in caso di smarrimento o furto di dispositivi.

Fate attenzione a transazioni e fatture fraudolente.

Le truffe possono spaziare da pagamenti con assegni a vuoto, carte di credito o debito fasulle a false restituzioni di merci. Stipulate un'assicurazione che vi tuteli da questi rischi. Inoltre, accertatevi che qualsiasi irregolarità venga immediatamente segnalata.

E-mail

Il provider di posta elettronica non può garantire la vostra sicurezza informatica e gli hacker attaccano i provider per ottenere l'accesso agli account degli utenti, oppure attaccano direttamente i singoli account e-mail con phishing, social engineering, malware o altre truffe.

Limitate la vostra esposizione creando account di posta separati per:

- azienda
- amici e famiglia
- messaggi d'allerta importanti siti che come ID utente richiedono un indirizzo e-mail

Inoltre, per tutelare i vostri dati:

- se disponibile, attivate nel vostro servizio di posta elettronica l'autenticazione a due fattori per ricevere un messaggio ad ogni accesso da un nuovo computer;
- utilizzate la crittografia per trasmettere i dati personali: le informazioni codificate non possono essere lette senza le apposite chiavi di cifratura;
- utilizzate filtri anti-spam per ridurre il rischio di software malevole e phishing (lo spam rappresenta il 65% di tutto il traffico e-mail);
- se dovete inviare a qualcuno un documento protetto da password, inviate il documento e la password con due e-mail separate.

Social Engineering

Il social engineering può esporvi al rischio di frode.
I social media, come Facebook o LinkedIn, rappresentano per gli hacker una ricca fonte di informazioni, che possono essere utilizzate per sottrarvi beni o dati.

- Riducete al minimo le informazioni divulgate online. I criminali setacciano Facebook, Twitter e altri social media per trovare dati personali, che utilizzeranno per frodare voi, la vostra famiglia e/o i vostri amici.
- Non inserite nelle e-mail informazioni di natura personale/finanziaria (e non seguite i link inviati nelle e-mail anche se provengono da fonti sicure).
- Contattate telefonicamente il mittente dell'e-mail o aprite una nuova finestra di posta (non rispondete con "rispondi") per chiedere al mittente se l'e-mail ricevuta è autentica.
- Prestate attenzione all'URL. I siti web malevoli si presentano esattamente come quelli legittimi, ma l'URL potrebbe contenere una variante ortografica o un dominio diverso (ad esempio, leggete .net al posto di .com?)
- Non inserite dati sensibili sui siti web a meno che il livello di sicurezza sia adeguato (l'URL deve iniziare con: https://).

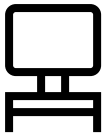
Al telefono
Se non conoscete l'interlocutore, verificate la sua identità: chiedete l'esatta grafia del nome, un numero di richiamata e il motivo per cui sono richieste le informazioni.

State in guardia da chi si presenta con identità fasulle: verificate la fonte tramite i canali pubblici ufficiali.

Non fornite informazioni su altre persone: se vi vengono richieste informazioni su un'altra persona, chiedete al chiamante di contattare direttamente la persona in questione.

Di persona
Nei luoghi pubblici, prestate attenzione agli "shoulder surfer" che vi osservano mentre inserite dati personali (come PIN o password) per rubarli e ottenere l'accesso ai vostri account.

- Non fidatevi di persone che cercano di accedere insieme a voi a un'area protetta, senza essere provvisti di autorizzazione (badge o token).
- Non inserite nel computer dispositivi di archiviazione rimovibili di origine ignota (ad esempio chiavette USB) che avete trovato o che avete ricevuto da altri, in quanto possono essere veicolo di malware.



Internet

HGli hacker ricreano noti siti web per impossessarsi delle credenziali degli utenti, come password, numeri d'assicurazione, dati di carte di credito, solo per citarne alcune. In seguito utilizzano le informazioni rubate per accedere alle vostre operazioni bancarie e ad altri account.

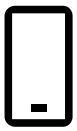
Alcune precauzioni da adottare online

- Accertatevi che il software del vostro browser sia aggiornato.
- Garantite un livello di sicurezza medio-alto nelle impostazioni del vostro browser.
- Verificate che l'indirizzo web di qualsiasi sito visitato inizi con https://. Accanto a https://, alcuni browser mostrano l'icona di un lucchetto, a indicare che la connessione è sicura.
- Attenzione: http:// non è sicuro.
- Dopo aver utilizzato un servizio bancario o di e-commerce su Internet, eseguite il logout per accertarvi che la sessione sia chiusa.
- Mantenete sgombra la cache dei cookies e del browser in modo che gli hacker non possano accedere al vostro storico per ottenere le informazioni.
- Tenete presente che sempre più spesso gli hacker prendono di mira i bambini sui social media e sui siti di giochi online.
- Attenzione ai siti che visitate: non accedete a siti che offrono download o contenuti illegali (ad esempio programmi di file sharing): anche se non scaricate i file, aprite la strada a virus che possono infettare il vostro computer.
- Bloccate le finestre pop-up e i contenuti pubblicitari; non rispondete ai pop-up che vi invitano a inserire o reinserire le vostre credenziali di accesso.

Migliori prassi

- Per individuare eventuali transazioni sospette, controllate regolarmente lo storico delle vostre operazioni bancarie e delle carte di credito, oltre agli estratti conto.
- Se possibile, avvaletevi sempre dell'autenticazione in due passaggi. Quando accedete a un bancomat automatica confermate la vostra identità con la carta e il PIN. Fate lo stesso online: per accedere al vostro account, utilizzate una password e un codice che vi verrà inviato via SMS, e-mail o chiamata. In questo modo, se qualcuno accede da un altro computer, riceverete un messaggio di allerta.
- Evitate di cliccare sul pulsante "chiudi" di un annuncio pubblicitario o in qualsiasi altro punto della finestra per chiuderla.
- Se possibile, attivate il browsing in incognito che previene l'archiviazione o il salvataggio dei cookies e della cronologia dei browser sul vostro dispositivo.
- Utilizzate segnalibri affidabili per i siti importanti, non link nella e-mail o pop-up.
- Chiudete le finestre che contengono annunci pop-up o avvertimenti indesiderati con la X nell'angolo in alto a destra.
- Non acquistate gli articoli pubblicizzati in un messaggio di spam: anche se si tratta di un'azienda legittima, il vostro acquisto incoraggia questa pratica.

Ricordate che ogni dispositivo rappresenta un rischio. Laptop, tablet e telefoni cellulari sono esposti a possibili violazioni della sicurezza wireless. Non collegatevi a siti che non vi sono familiari o noti. Non date per scontato che un link Wi-Fi sia sicuro; gli hacker generano punti di accesso fraudolenti che appaiono esattamente come quelli legittimi. Utilizzate invece una rete virtuale privata (VPN) che consente l'accesso solo agli utenti autorizzati, in modo che i dati non vengano intercettati.



Sicurezza mobile

Dipendiamo sempre più dai nostri smartphone e tablet per effettuare operazioni bancarie, fare shopping e accedere ai social network; ecco perché è essenziale proteggere i dispositivi mobili. Tutti dovrebbero adottare misure atte a garantire la sicurezza di questi dispositivi.

Guida alle migliori prassi per i vostri dispositivi personali

- Definite le impostazioni di sicurezza in modo da limitare l'accesso di terzi ai vostri dati tramite connessioni wireless e Bluetooth.
- Evitate di cliccare sulle pubblicità di Internet: esistono app per bloccare gli annunci pubblicitari sia per dispositivi Android che per dispositivi Apple e le impostazioni del browser possono essere configurate in modo da limitare l'ad tracking.
- Aggiornate le app sul vostro dispositivo non appena sono disponibili nuove versioni, poiché queste ultime spesso contengono patch di sicurezza.
- Se sospettate che il vostro dispositivo sia stato infettato da malware: contattate il fabbricante o il gestore di telefonia mobile per richiedere assistenza.
- Installate un'app di sicurezza per scansionare e rimuovere le app infettate da malware.
- Non cercate di aggirare i controlli di sicurezza nel sistema operativo del dispositivo (ad esempio. non effettuate procedure di jailbreaking o rooting del telefono).
- Tenete il telefono o il computer bloccato: assicuratevi che sia sempre protetto da password e PIN.
- Tenete costantemente aggiornato il software del sistema operativo e assicuratevi di avere installato le patch di sicurezza più recenti.
- Codificate Cifrate le informazioni sensibili: se il vostro dispositivo mobile o laptop offre funzioni di crittografia, usatele.
- Controllate le app sul vostro telefono: tenete traccia delle richieste di permessi/accessi dalle app installate sul vostro dispositivo.
- Utilizzate un programma anti-malware/virus affidabile e aggiornatelo costantemente. I dispositivi mobili sono esposti agli stessi rischi dei computer installati in casa o in ufficio.
- Disattivate Bluetooth quando non vi occorre la connessione: il vostro dispositivo sarà meno vulnerabile agli attacchi informatici ed evitate di consumare la batteria.
- Scegliete uno smartphone con funzioni di sicurezza antifurto. In caso di smarrimento o furto del telefono, la funzione di accesso remoto vi consentirà di bloccarlo, cancellare l'archivio dei dati e identificarne la posizione.
- Effettuare regolarmente il backup dei vostri dispositivi sul computer di casa o sulla rete cloud in modo da preservare l'accesso alle informazioni in caso di smarrimento, furto o danneggiamento del dispositivo.
- Le organizzazioni criminali utilizzano il malware per rubare o distruggere i vostri dati: così facendo, pregiudicano la sicurezza e l'integrità delle attrezzature e/o dei sistemi di cui vi servite. Non ignorate gli avvertimenti. Installate software antivirus e prestate attenzione agli avvertimenti, ad esempio quando cercate di accedere a un sito non sicuro su Internet.
- Procedete con cautela per ciò che cliccate e scaricate. Aprendo link sconosciuti, vi esponete al rischio di programmi software malevoli in grado di scansionare il vostro computer o tenere traccia dei tasti digitati, come password e numeri di conto.
- Alcuni programmi integrano intenzionalmente software malevolo. Durante l'installazione prestate attenzione alle caselle di messaggio e alle scritte in caratteri minuti. Annullate l'installazione se ritenete che possa essere dannosa.
- Diffidate delle e-mail sospette. Anche le e-mail provenienti da mittenti noti possono contenere link o allegati di malware se il loro account è stato corrotto.
- Sospettate dei link presenti nella posta in arrivo. Se possibile, visitate i siti web inserendo l'indirizzo desiderato direttamente nel browser.
- Prima di aprire i file, eseguite una scansione con il software di sicurezza. Non date per scontata la sicurezza dei file inviati per e-mail o di quelli trasferiti da disco o unità flash.

Malware

Diffidate delle finestre pop-up che vi invitano a scaricare programmi software. Il loro obiettivo è convincervi che il computer è stato infettato e che il problema si risolverà scaricando il software. Chiudete immediatamente questa finestra, avendo cura di non cliccare al suo interno.

- I siti di file sharing sono in gran parte illegali e vanno evitati. Questa tipologia di servizio non offre una protezione adeguata contro il malware, che può nascondersi in un noto film, un album o un programma.
- Non perdete la calma se il vostro computer è stato infettato con un virus ransomware: una finestra pop-up vi informa che i file sono stati cifrati e saranno sbloccati solo in cambio di un riscatto in denaro. Scollegate immediatamente il dispositivo dalla rete e tentate di ripristinare i file da una precedente copia di backup integra. Non pagate il riscatto.

CREDIT SUISSE AG
Casella postale 100
CH-8070 Zurigo
credit-suisse.com

MCIZ 02.2019