Baloise DIGITAL SCOUTS

Cyber Security Guide – per persone private

Vi mostriamo la strada attraverso la giungla digitale.

www.baloise.com/digitale-pfadfinder

Baloise Group

Informazioni sugli scout digitali

La truppa degli scout digitali di Baloise Group è composta da collaboratori motivati e interessati. Come ambasciatori della digitalizzazione, offrono un aiuto per riuscire a trovare la giusta strada nella giungla digitale. L'organizzazione degli scout digitali Baloise nasce da una collaborazione tra Group IT e Public Affairs.

Obiettivo e scopo degli scout digitali
Gli scout digitali Baloise forniscono un contributo facoltativo nell'ambito di Corporate Social Responsibility di Baloise, poiché le esigenze della società vanno oltre l'acquisto di prestazioni di sicurezza. I collaboratori Baloise dispongono di un vasto know-how che viene messo a disposizione della società al di là delle prestazioni di servizio rilevanti per l'attività aziendale.

Avete interesse a partecipare ad uno dei nostri eventi informativi sul tema cyber security?
Scriveteci un'e-mail:
pfadfinder@baloise.com

Introduzione

Questa brochure ha lo scopo di aiutarvi a essere informati in merito ai rischi ed ai pericoli che si celano nell'uso quotidiano di Internet nella vostra vita privata. Inoltre, essa vi spiega quali sono le basi della cyber security presentando delle direttive preventive per evitare di incappare proprio in questi pericoli.

I rischi a livello di cyber security sono presenti sotto molte forme e possono provocare danni di dimensioni e portata devastanti. Il principale punto debole nella sicurezza IT, che sia a casa o in ufficio, è e rimane sempre la persona stessa. Una chiara comprensione dei rischi e delle conseguenze del proprio agire può però contribuire in modo evidente a limitare la possibilità di fare errori.

I termini principali in breve

Social engineering
È “l’arte” di manipolare le persone allo scopo di indurle ad adottare un certo comportamento, ad esempio, vista la buona fede di una determinata persona, si cerca di manipolarla in modo tale da farsi confidare informazioni riservate. Facendo appello alla disponibilità delle vittime, il social engineer cerca di procurarsi l’acceso a dati sensibili.

Malware
Termine generale che indica i software che eseguono funzioni indesiderate e dannose. Il malware spesso non si diffonde da solo, bensì utilizza un programma ospite e, facendo leva sull’utilità di esso, cerca di indurre l’utente a installarlo. I programmi malware più conosciuti sono i trojan, gli spyware e i ransomware.

Phishing
Tentativi di accedere ai dati personali di utenti Internet attraverso l’uso di siti Internet, e-mail o messaggi falsi allo scopo di danneggiare le persone coinvolte (ad esempio furto di dati o di valori pecuniari). Il phishing è una forma particolare di social engineering.

Distributed Denial of Service (DDoS)
Blocco dei servizi informatici esposti a Internet (sito web, negozio online o forum), causato da un’enorme quantità di richieste. Questo blocco impedisce l’utilizzo del servizio informatico mirato. Questo tipo di attacco può essere causato da sovraccarichi involontari o da un attacco mirato. Si tratta di una forma di ricatto che sta diventando sempre più comune nell’era del business online.

Cybermobbing
Termine generale che indica quei comportamenti volti a diffamare e importunare altre persone o imprese avvalendosi dell'uso di Internet o di dispositivi mobili. Fa parte del cybermobbing anche il furto di identità, ad esempio allo scopo di svolgere transazioni o rilasciare affermazioni a nome di altri. Si tratta anche qui di una forma particolare di social engineering.

Ransomware (dall'inglese "ransom" per "riscatto")
Chiamati anche cryptolocker o virus del riscatto, sono programmi di malware con cui l'intruso riesce ad accedere a determinati dati per poi bloccare l'utilizzo di essi o l'accesso a tutto il sistema informatico. Lo scopo è estorcere denaro per poter riacquisire l'accesso ai propri dati. Nel 2017 gli attacchi dei malware WannaCry e NotPetya hanno ottenuto risonanza a livello mondiale mettendo completamente k.o. tra gli altri anche ospedali e aziende di logistica.

Sensibilizzazione
Password e sicurezza

Le password non andrebbero mai scritte e non dovrebbero mai essere comunicate a nessuno. L'autenticazione a più fattori è un metodo buono e semplice per aumentare la sicurezza di un account. Ad esempio, al momento del login viene inviato all'utente un SMS al numero di cellulare registrato, contenente un codice numerico per poter proseguire con la procedura di login. Per ogni account dovrebbero essere utilizzate password diverse, non troppo simili tra loro. È necessario essere consapevoli del fatto che le password possono andare perse e che quindi è bene cambiarle regolarmente. È molto importante quindi non cambiare solo un numero o una lettera, bensì utilizzare una password completamente nuova.

In caso di sospetto di uso illecito dell'account, è fondamentale modificare subito la rispettiva password.

Cassaforti per password

Le cosiddette cassaforti per password (password vault) servono a semplificare la creazione e la memorizzazione di password nuove ed esistenti. Si tratta di applicazioni che permettono di generare una password sicura e di salvarla in combinazione con un account. L'applicazione stessa viene protetta grazie ad una complessa master password, sullo smartphone, anche tramite identificazione con impronta digitale o riconoscimento facciale. In questo modo dovete ricordarvi solo la master password e poi potete consultare tutte le altre password. Ecco alcuni buoni esempi di cassaforti per password: SecureSafe, 1Password e Keeper Security.

Checklist per la sicurezza delle password

- ☐ Almeno otto caratteri
- ☐ Maiuscole e minuscole
- ☐ Numeri e caratteri speciali
- ☐ Nessuna combinazione di lettere contenuta in dizionari
- ☐ Password mai usata prima

Suggerimento:

Se non doveste utilizzare alcuna cassaforte per password, espedienti mnemonici e frasi per password possono aiutare a creare nuove password e quindi a ricordarle più facilmente. Si tratta di frasi semplici che permettono di creare una password utilizzando, ad esempio, le prime lettere di ogni parola.

Esempio:

→ Frase d'esempio per la creazione di una password: Mio figlio è nato nel febbraio 1994, compie 26 anni quest'anno.

→ Ogni prima lettera o numero in ordine, rispettando le maiuscole e le minuscole:

Mio figlio è nato nel febbraio 1994, compie 26 anni quest'anno.
→ Password: **Mfennf94$c26aq$a**

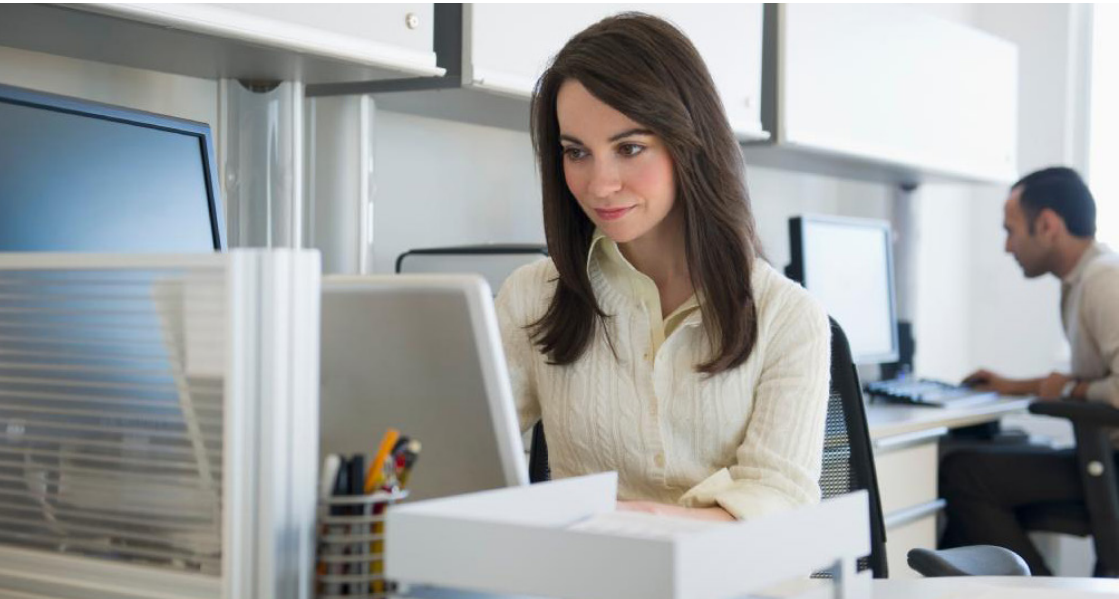
Social engineering
Esempio e comportamento da seguire

Il social engineering può essere praticato nei vostri confronti durante una conversazione diretta, ma anche online oppure al telefono. I seguenti esempi e le azioni consigliate hanno lo scopo di aiutarvi a riconoscere un certo schema ricorrente.

Situazione: un principe nigeriano vi contatta tramite e-mail perché desidera consegnare oro in Svizzera per un valore di molti milioni di franchi. Voi dovreste aiutarlo in veste di intermediario e potrete poi tenere per voi una certa quota del ricavo totale.

→ Suggerimento di azione: un classico che purtroppo funziona ancora troppo spesso. Se qualche sconosciuto vi promette un buon profitto tramite Internet, potete essere certi che si tratta di una truffa. Non rispondete a questa e-mail, bensì cancellatela direttamente.

Situazione: la persona con cui avete concordato un appuntamento online, e che non avete ancora incontrato personalmente, scrive che ha problemi familiari e che ha bisogno di denaro da voi



per pagare il viaggio nel proprio paese, spesso tramite l'acquisto di crediti per carte prepagate MasterCard.

→ Comportamento consigliato: non date più ascolto a questo individuo. Quasi sicuramente non si tratta della persona che ha detto di essere sul portale online, probabilmente nemmeno del sesso indicato. Bloccate e indicate questa persona agli amministratori del portale, così che possa essere eliminata dalla piattaforma.

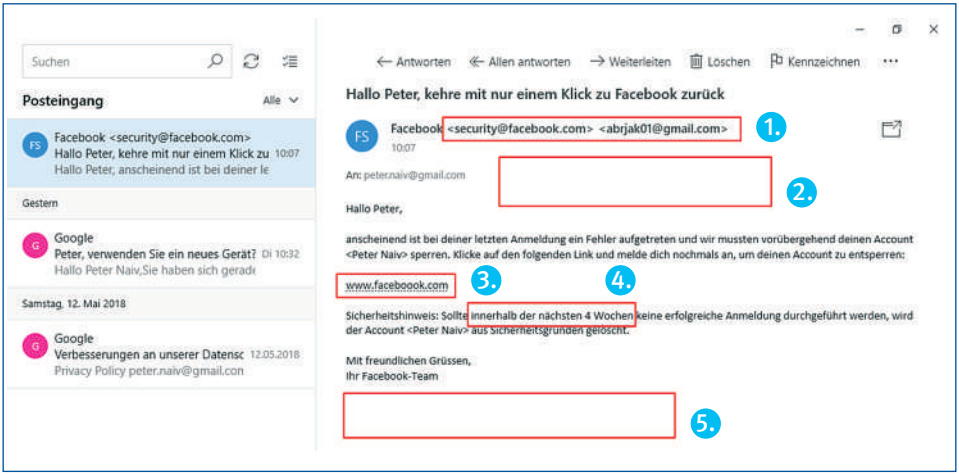
Situazione: l'interlocutore al telefono si presenta come collaboratore dell'Helpdesk di un produttore di hardware come HP, Dell o Apple e vi informa che si è verificato un problema con il vostro dispositivo. Successivamente vi invita a rivelare vari dati e dettagli personali sul vostro dispositivo e sulla vostra connessione Internet.

→ Comportamento consigliato: non fornite alcuna informazione dettagliata sulla vostra persona o sui vostri dispositivi se venite chiamati, ma riattaccate. I produttori di hardware non hanno possibilità di riconoscere automaticamente se e come funziona il vostro dispositivo acquistato e se si verificano problemi, voi dovete chiamare l'Helpdesk del produttore.

Situazione: nella chat del vostro videogioco online qualcuno si presenta come amministratore e vi informa che il vostro account è corrotto. Per ripristinarlo, prima di perdere importanti dati di gioco, questa persona ha bisogno della vostra password e dell'indirizzo e-mail con cui vi siete registrati al gioco.

→ Comportamento consigliato: ignorate questa persona e bloccatela o indicatela a chi di dovere, se possibile. Nessun amministratore di un gioco vi scriverebbe nella chat del gioco stesso per discutere i problemi del vostro account: tali comunicazioni avvengono sempre tramite uno scambio di e-mail. Di norma, i produttori del gioco informano sempre in prima persona che nessuno dei loro amministratori richiederebbe dati personali in chat. Ignorate inoltre anche tutti i messaggi in chat che vi offrono grandi quantità di "valuta in-game" a un prezzo vantaggioso: anche in questo caso si tratta sempre di una truffa.

Phishing
Esempio e comportamento da seguire



Con l'e-mail sulla destra si spiega con un semplice esempio come riconoscere un'e-mail di phishing e come comportarsi nel modo giusto.

Fattori di riconoscimento (riquadri rossi) dall'alto verso il basso.

1. Il mittente indicato ha due indirizzi e-mail, il secondo dei quali non sembra assolutamente essere quello di un impiegato di Facebook.
2. Manca il logo Facebook. Tutta la e-mail non ha il solito formato tipico di Facebook.
3. Il link indicato per accedere a Facebook contiene una "o" di troppo. Inoltre, il link stesso non sembra assolutamente indirizzare verso una pagina di login o di sblocco della pagina.

4. La questione sembra essere un po'urgente. La stessa frase contiene anche una minaccia sotto forma di possibile cancellazione dell'account.

5. Mancano il classico disclaimer e la nota sulla protezione dei dati a fine e-mail. Non sono neppure indicate le opzioni di presa di contatto con il support di Facebook. Se in seguito l'account dovrebbe essere veramente cancellato, qui sarebbero sicuramente riportate delle informazioni di contatto.

Altre caratteristiche tipiche di un'e-mail di phishing:
- → Formulazioni impersonali
- → Errori di battitura e problemi con gli accenti
- → Uso di una lingua inconsueta (ad esempio l'inglese sebbene utilizziate il servizio in italiano)
- → Diversi tipi di formattazione nell' e-mail

Cifre e fatti:
45 % degli utenti Internet cliccano sui link contenuti nelle e-mail di mittenti sconosciuti.
92 % di tutti gli attacchi hacker iniziano con un'e-mail di phishing.

Come comportarsi con le e-mail di phishing?
Non tutte le e-mail di phishing sono identificabili a prima vista. In caso di sospetto, potete procedere nel seguente modo:
- → Cancellare l'e-mail; se dovesse trattarsi effettivamente di un'e-mail importante, il vero servizio online vi contatterà.
- → Verificare manualmente (senza cliccare sul link all'interno dell'e-mail) lo status del profilo o del servizio.
- → Chiamare il supporto clienti del mittente e chiedere informazioni. Il numero di telefono del supporto clienti di un fornitore di servizi si trova facilmente con una ricerca su Google.

Ricordate che nessuna azienda seria informerebbe i propri clienti della cancellazione dell'account solo tramite e-mail. In particolar modo gli istituti finanziari e assicurativi vi informeranno per prima cosa telefonicamente e via posta se dovessero verificarsi problemi con il vostro account.

SMS Phishing

Il phishing può avvenire anche tramite un SMS sul cellulare.
Controllate sempre quando ricevete un SMS con un link, alcuni consigli importanti per riconoscere un tentativo di phishing:

- → Controllare il nome e il numero del mittente
- → Controllare l'ortografia del messaggio
- → Guarda il link (ad es. il nome dell'azienda scritto correttamente)
- → In caso di dubbio contattare il servizio clienti dell'azienda per telefono o per e-mail.

Protezione da ransomware
e reazione in caso di attacco

Il ransomware può accedere in diversi modi al vostro sistema e danneggiarvi con il blocco dei vostri dati. Tenete a mente le seguenti misure per evitare questo tipo di ricatto.

→ Attenzione alle e-mail, soprattutto all'apertura di allegati. I ransomware vengono trasmessi soprattutto tramite e-mail e si propagano all'interno del vostro sistema nel momento in cui cliccate su un link o scaricate un allegato. Usate assolutamente un antivirus per verificare gli allegati di mittenti sconosciuti prima di aprirli.

→ Attenzione ai dispositivi di memorizzazione come le chiavette USB e i dischi rigidi portatili. Soprattutto se non conoscete l'utente precedente del dispositivo e non siete completamente sicuri del contenuto del dispositivo stesso, non dovreste mai collegarlo al vostro sistema.

→ Mantenete sempre aggiornati i vostri sistemi. Le nuove versioni dei sistemi operativi contengono spesso miglioramenti in fatto di sicurezza. Anche gli aggiornamenti del programma antivirus contengono miglioramenti per il riconoscimento e la difesa antivirus e dovrebbero essere fatti regolarmente.

Ricordate che il ransomware spesso è programmato in modo da diffondersi ulteriormente nella rete infetta: ciò significa, ad esempio, che tutti i dispositivi collegati alla vostra WLAN sono potenzialmente prossime vittime del ransomware.

→ Utilizzate quindi una soluzione di backup per tutti i dispositivi presenti nella vostra casa e create regolarmente copie di sicurezza dei vostri dati e di quelli dei vostri coinquilini.

In caso di attacco

→ Non pagate il riscatto richiesto! In questi casi spesso poi il riscatto viene aumentato ed i dati rimangono criptati.

→ Rivolgetevi a un professionista e cercate di ripristinare il sistema con una versione di backup precedente all'attacco.

Ulteriori direttive preventive importanti

Informare familiari e coinquilini
Se abitate in una casa con più dispositivi abilitati all'accesso a Internet e con più utenti, informate questi ultimi circa i rischi di Internet e scambiatevi consigli a vicenda. Spesso bambini ed i ragazzi sanno più su Internet di quanto si creda. Ciononostante è consigliabile concordare insieme una soluzione con regole di condotta per l'uso della rete.

Salvataggio dati – esecuzione di backup
I vostri dati possono andare persi e non solo nel caso di un attacco hacker. Anche altri fattori esterni come l'incendio o i danni da acque ed il danneggiamento fisico del dispositivo possono provocare la perdita di dati.
Ricordate pertanto di fare regolarmente delle copie di sicurezza dei vostri dati, i cosiddetti backup. Anche in questo caso sono in vendita programmi di diversa qualità e di diverso prezzo. L'importante è che verifichiate regolarmente che i dati salvati possano essere ripristinati. Inoltre, i backup non dovrebbero essere conservati nello stesso dispositivo e nello stesso luogo usato per i dati originali. Acquistate un disco rigido esterno o utilizzate una soluzione di backup che salvi i vostri dati in un cloud. Ricordate però, nel caso scegliate la soluzione di backup con cloud, che a seconda della sede dell'azienda, le leggi sulla protezione dei dati possono essere diverse da quelle della Svizzera.
Consigliamo inoltre l'uso di un firewall per difendervi dagli attacchi esterni nonché l'installazione di un antivirus che verifichi regolarmente l'eventuale presenza di aggressori nel vostro sistema e nei file in esso presenti.

La maggior parte dei programmi antivirus, di firewall e di backup offre una versione di test oppure è completamente gratuita. Pertanto vi consigliamo di prendervi il tempo necessario per testare alcuni programmi e scegliere una soluzione adeguata nel prezzo e nelle prestazioni al vostro budget ed alle vostre esigenze.

Aggiornare sistemi operativi e programmi
Ricordate di eseguire regolarmente e frequentemente gli aggiornamenti di assistenza e sicurezza per il proprio sistema operativo e i programmi in uso. Queste patch chiudono le falle e le lacune note, aumentando così la sicurezza per tutte le funzioni utilizzate.
Tutti i sistemi operativi e programmi per computer o smartphone hanno degli errori. Gli autori di malware sfruttano queste falle per penetrare nel computer o nello smartphone. Vale quindi la pena utilizzare, oltre ai servizi standard di sicurezza del vostro sistema operativo (ad esempio Windows Defender), soluzioni antivirus e firewall integrative.

Buon senso
Quando navigate in Internet o eseguite delle operazioni con dati sensibili, affidatevi sempre al vostro buon senso.

Per ulteriori linee guida preventive, informazioni in merito alla cyber security e interessanti attacchi hacker dal vivo, partecipate agli eventi informativi ed alle presentazioni degli scout digitali di Baloise.

L'attività di hacker è punibile
Qualsiasi tipo di attacco hacker è proibito dalla legge.

Sostegno statale
Dal 2010, lo Stato offre la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) su www.melani.admin.ch**, dove trovate informazioni in merito ai pericoli e alle misure attuali, come anche un modulo di annuncio per attacchi.**

Have I Been pwned?
Il servizio web Have I Been pwned (HIBP) raccoglie e analizza i cosiddetti data dumps che gli hacker mettono in rete dopo aver messo a segno i loro data breach. HIBP offre agli utenti la possibilità di verificare se, in questo mare di informazioni rese note e quindi non più protette, si trova anche il proprio indirizzo e-mail o il proprio user name. Inoltre è possibile impostare anche una funzione con la quale si viene informati tramite e-mail in caso i propri dati dovessero essere resi noti in un data breach. È inoltre possibile cercare tra le password rese pubbliche. Per questo motivo è importante utilizzare più password, poiché quelle rese note nei data breach vengono vendute in Internet e non possono quindi essere più utilizzate.
https://haveibeenpwned.com

Baloise Group
Aeschengraben 21
CH-4002 Basel
pfadfinder@baloise.com

www.baloise.com

000.1039i 5.20 100