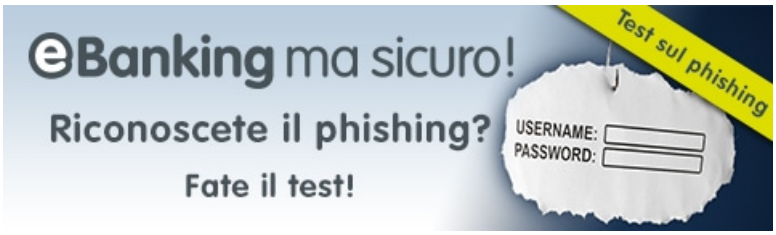
Phishing

Per mezzo del phishing i malintenzionati cercano di carpire i dati d'accesso di ignari utenti Internet, p. es. per accedere ai portali di e-banking o agli shop online. I criminali dissimulano una falsa identità e sfruttano così la buona fede delle loro vittime.

Proteggetevi dal phishing così:

- Non utilizzate mai un link ricevuto via e-mail, messaggio breve o servizio di messaggistica o scansionato tramite codice QR per accedere a un istituto finanziario.
- Non compilate mai i moduli ricevuti via e-mail o messaggio breve che chiedono di inserire i dati d'accesso.
- Gestire con grande prudenza gli allegati delle e-mail e dei servizi di messaggistica breve.
- Durante le telefonate non comunicate mai informazioni riservate come le password.
- Inserite l'indirizzo della pagina di accesso del vostro fornitore di servizi online o istituto finanziario sempre manualmente, nella barra degli indirizzi del browser.
- Quando aprite la pagina di accesso, verificate che la connessione sia TLS (https://, icona a forma di lucchetto) e assicuratevi di trovarvi sulla pagina desiderata controllando l'indirizzo Internet nella barra degli indirizzi del browser.
- In caso di incertezze o dubbi rivolgetevi al vostro istituto finanziario.



(https://www.ebas.ch/it/test-sul-phishing/)

Come funziona un attacco di phishing tipico

1. Contatto

I criminali inviano e-mail falsificate spacciandosi per dipendenti di fornitori di servizi online o istituti finanziari. Ai destinatari delle e-mail, per esempio, viene segnalato che i dati del conto o le credenziali d'accesso (p. es. nome utente e password) non sono più sicuri o aggiornati e vanno corretti cliccando sul link contenuto nell'e-mail.

2. Intercettazione dei dati personali

Tuttavia, il link non apre la pagina originale del fornitore di servizi indicato, ma una pagina Internet contraffatta che però sembra originale. Le informazioni personali che vengono inserite su questo sito, come le password, arrivano direttamente ai criminali.

3. Arricchimento
I criminali utilizzano quindi le informazioni rubate per effettuare, a nome delle vittime, trasferimenti bancari, acquisti online od offerte false sui siti delle case d'aste online.

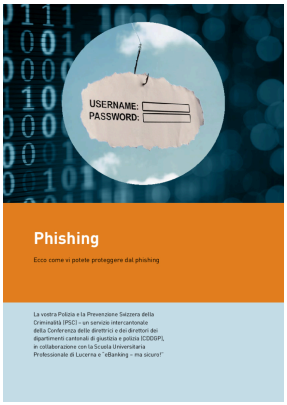
Per inviarvi e-mail di phishing, i truffatori devono conoscere il vostro indirizzo e-mail. Per ridurre questo rischio e in generale anche l'afflusso dello spam nella vostra posta in arrivo, è utile seguire alcune semplici regole che potete trovare nel nostro articolo sullo spam (https://www.ebas.ch/it/protezione-contro-lo-spam/) .

(https://www.antiphishing.ch/it/)

Per «phishing» si intende il furto di informazioni preziose, come le credenziali d'accesso di utenti Internet.

Il termine è una parola inglese inventata sulla base di «password» e «fishing».

Promemoria:



(https://www.ebas.ch/wp-content/uploads/2019/10/phisingSKP_it.pdf)

Maggiori informazioni

Phishing classico

Nel phishing classico i malintenzionati cercano di attirare le loro vittime su siti falsificati per mezzo di e-mail contraffatte, spingendole così a inserire le loro credenziali d'accesso (come il numero di contratto o la password) su queste pagine.

In alternativa o in aggiunta a questo, spesso vengono inviati via e-mail degli allegati contenenti cavalli di Troia che una volta aperti si installano in background e da quel momento in poi spiano i dati d'accesso dell'utente Internet o lo portano su siti Internet contraffatti.

È importante sapere che gli istituti finanziari non inviano mai messaggi di questo tipo!

Prevenzione: non fare clic su nessun link o allegato di un'e-mail, ma inserire sempre l'indirizzo dell'istituto finanziario manualmente nel browser. Verifica della connessione TLS e del certificato (https://www.ebas.ch/it/verifica-del-certificato/) .

Spear phishing e dynamite phishing

Diversamente dal phishing classico, con il quale si inviano grandi quantità di e-mail a un numero enorme e indiscriminato di destinatari, lo spear phishing seleziona i destinatari in modo mirato e invia messaggi personalizzati.

Il mittente si spaccia per una persona affidabile, spesso un conoscente, collaboratore o partner commerciale del destinatario. Il contenuto delle e-mail personalizzate ha un aspetto credibile e autentico e quindi spesso non viene riconosciuto dai filtri antispam.

Se le e-mail personalizzate vengono create automaticamente e inviate in massa, si parla anche di «dynamite phishing».

Prevenzione: siate diffidenti quando ricevete delle e-mail inattese o dal contenuto insolito, anche se pensate di conoscere il mittente. In caso di dubbio contattate il mittente usando un canale diverso, p. es. il telefono.

Smishing (phishing via SMS)

Anche i messaggi SMS vengono usati sempre di più per sferrare attacchi di phishing. Il lato più perfido dello «smishing» è che con i messaggi SMS non è possibile applicare la maggior parte dei criteri utili per riconoscere le e-mail di phishing. Per esempio, è molto raro leggere un appellativo personale. Il linguaggio e la struttura dei messaggi di testo sono troppo semplici e concisi per permettere di trovare segnali di un'eventuale contraffazione. E con la maggior parte dei dispositivi mobili è difficile se non impossibile verificare chi sia il vero mittente e quale la destinazione del link. Oltre a questo, molti utenti sono abituati a ricevere messaggi SMS per verificare il proprio accesso all'e-banking o validare transazioni finanziarie.

Prevenzione: non fate mai clic sui link contenuti nei messaggi SMS, ma digitate manualmente nel browser l'indirizzo noto del sito Internet dell'istituto finanziario controllando che la connessione sia sicura (icona a for-

ma di lucchetto, indirizzo di destinazione). Se ricevete messaggi SMS inattesi, contattate la banca ai recapiti che conoscete (p. es. al numero di telefono ufficiale) e chiedete conferma dell'invio del messaggio.

Vishing (voice phishing)
Il vishing è la variante orale o telefonica del phishing. Come nel phishing classico gli utenti vengono indotti mediante storie ben congegnate a condividere informazioni riservate come i dati di accesso al sistema di e-banking.

Prevenzione: non comunicate mai a un'altra persona dati riservati come le password. Interrompete subito le telefonate in cui vi chiedono questi dati. Per contattare il vostro istituto finanziario utilizzate esclusivamente i numeri di telefono ufficiali.

Phishing QR
Nel phishing QR i malintenzionati incollano i propri codici QR (Quick Response Codes) sopra ad altri codici ubicati in luoghi molto frequentati conducendo così gli utenti a un indirizzo URL sbagliato. Questo permette loro, soprattutto su dispositivi mobili, di avviare immediatamente dei download, eseguire degli script o aprire una pagina contraffatta per l'accesso a un istituto finanziario.

Prevenzione: non utilizzate mai un codice QR per accedere a un istituto finanziario. Prima di scansionare un codice QR verificate che non sia stato coperto da un codice contraffatto. Controllate che il link apra l'indirizzo desiderato.

Phishing con pagine Internet in allegato
Quando il phishing avviene tramite pagine Internet, nelle e-mail non si trovano né link né documenti, ma piuttosto una pagina Web contraffatta allegata come file HTM o HTML. La vittima viene tratta in inganno dal fatto che non ci sia più un link da cliccare. Oltre a questo, anche aprire il file allegato sembra non comportare particolari rischi, visto che non si tratta di un documento (Word, Excel ecc.) che potrebbe eseguire macro, ad esempio.

Attenzione però! I file HTM e HTML possono reindirizzare la vittima direttamente al server del malintenzionato! Le credenziali inserite, quindi, finirebbero nelle mani sbagliate. Inoltre, in quei file si potrebbero trovare anche script capaci di causare ulteriori danni.

Nei moderni programmi di posta elettronica, tali reindirizzamenti e script vengono bloccati per motivi di sicurezza. Tuttavia, quando si apre un allegato HTM o HTML la pagina Internet esce dal controllo delle impostazioni di sicurezza di tali programmi. La perfidia più insidiosa è che vengono ingannati anche gli utenti più sensibilizzati, perché nella barra degli indirizzi del browser compare «solo» un percorso file locale e non un URL sospetto, come avviene con il phishing classico.

Prevenzione: in generale, trattate con scetticismo gli allegati HTM e HTML. Non fate clic sugli allegati delle e-mail, ma inserite sempre manualmente l'indirizzo dell'istituto finanziario nel browser.