con la collaborazione di

Google™

SICURAMENTE ONLINE

PROTEGGI GLI **ACCOUNT** PERSONALI

PENSI CHE IL **PHISHING**
SIA SOLO UN TIPO DI PESCA?

PENSI CHE I **COOKIE**
SIANO SOLO BISCOTTI?

PENSI CHE UN **VIRUS**
SIA SOLO UN RAFFREDDORE?

PROTEGGI GLI **ACCOUNT** PERSONALI

È molto importante proteggere gli account personali, in quanto un utilizzo da parte di terzi potrebbe comportare seri rischi, che potrebbero sfociare ad esempio nel **furto d'identità**, consistente nell'utilizzo illecito di dati personali della vittima, senza che la stessa ne sia a conoscenza. In particolare, il furto d'identità può essere attuato per:
- utilizzare i dati personali di un soggetto o di un'impresa per ottenere prestiti finanziari, crediti, aprire conti correnti intestati alla vittima;
- prelevare denaro dal conto del soggetto;
- effettuare acquisti o transazioni a nome della vittima;
- impersonificarsi, tramite la rete, nella vittima, allo scopo di veicolare messaggi dal contenuto solitamente disdicevole (ad. Es. attività di cyberbullismo).

Per quanto concerne la sicurezza degli account personali, oltre ai consigli elencati nella sezione "Proteggi le tue password" è utile adottare alcuni accorgimenti:

- Utilizzo di servizi crittografati

È consigliabile usare servizi che supportino la crittografia SSL: protocollo che configura un percorso di comunicazione protetto tra computer. Se il servizio che stai utilizzando supporta la crittografia SSL, i dati inviati a e dal sito dovrebbero essere protetti dai malintenzionati. I servizi che utilizzi hanno questo servizio se:
- l'indirizzo inizia con https;
- nella barra in fondo al tuo browser compare una piccola icona di un lucchetto.

La crittografia SSL è necessaria nelle pagine web con accesso ai dati personali come nome e cognome, indirizzo, codice fiscale, codice della carta di credito ecc. Esempi di pagine in cui è fondamentale questa funzione sono quelle delle banche con accesso all'area

personale, siti di compravendita online, caselle di posta elettronica contenenti dati importanti.
Prima di inserire i tuoi dati su un sito controlla sempre che la pagina web sia crittografata!

- Connessioni sicure
È inoltre sconsigliato accedere ad un account personale quando si è connessi a reti WiFi pubbliche e libere. In particolare, sarebbe opportuno non digitare la password, in quanto non puoi sapere se la rete utilizzata è sicura. Ci sono programmi chiamati "sniffer di rete", che vengono usati dagli hacker per intercettare il traffico di dati;

- Attenzione ai siti fake
Il sito fake (dall'inglese "fake": "falso") è una pagina web finta, identica - per quanto riguarda la grafica e i contenuti - a quella di un sito originale, ma che ha piccolissime differenze nell'indirizzo, come ad esempio un punto o una lettera (ad es. il sito fake di www.adoc.org potrebbe essere www.a.doc.org).Il sito fake viene utilizzato dai malintenzionati per rubare i dati dell'utente.
I malintenzionati possono farti arrivare alla pagina fake tramite diverse strategie (attraverso un link inviato tramite e-mail o messaggi privati, ecc.).
Questa tecnica offre la possibilità di rubare le credenziali di accesso di ogni sito web che richieda l'autenticazione degli utenti attraverso username e password.
Alla luce di quanto detto è opportuno controllare sempre i siti che prevedono l'accesso all'area personale tramite password prima di inserire i dati: verifica che l'indirizzo sia scritto correttamente;

- Attenzione alle truffe di phishing
Il phishing è un tipo di truffa informatica finalizzata **all'acquisizione, per scopi illegali, di dati riservati**. Il phisher manda alle ipotetiche vittime e-mail che sembrano provenire da siti commerciali o istituzioni come le Poste o la propria banca, nelle quali vengono

richiesti dati personali. Il phisher può anche rimandare l'utente, tramite un link, a un sito fake, in cui **gli si chiede di inserire i dati personali o le password** per l'accesso all'area personale del sito falsificato.
In generale bisogna diffidare sempre dalle comunicazioni da parte delle istituzioni via e-mail, in quanto **queste ultime non utilizzano tale mezzo per richiedere dati sensibili.** Quando ricevi **una e-mail che chiede dati personali, è sempre una truffa**.
Altri esempi di phishing sono:
- e-mail inviate dal gestore di posta elettronica utilizzato, che chiedono di rispondere inviando i tuoi dati personali o di accesso alla casella;
- e-mail che chiedono soldi con promesse di vincere grosse somme di denaro;
- e-mail che invitano a pagare qualcosa che non è mai stato comprato;
- e-mail recanti offerte di lavoro e/o di collaborazione da parte di società sconosciute.

In generale, è bene:
- non inviare mai dati personali quali coordinate bancarie, password ecc. via e-mail;
- non inserire mai la tua password dopo aver cliccato su un link contenuto in un'e-mail. Accedi al sito direttamente dal web digitandone l'indirizzo;
- verificare che l'anti-virus blocchi i siti di phishing o installare una barra degli strumenti del browser che segnali eventuali attacchi di phishing;
-segnalare le frodi di phishing. Quasi tutti i fornitori di servizi e-mail consentono di segnalare episodi di phishing e e-mail sospette. La segnalazione bloccherà l'invio di altre e-mail da parte del mittente e consentirà ai team che si occupano dei comportamenti illeciti di fermare simili attacchi;

- Social network, social forum e blog: qualche attenzione in più

Particolare attenzione va poi posta ai social network, social forum e blog. Se da un lato offrono l'opportunità di creare reti sociali, condividere interessi e accrescere le proprie conoscenze, dall'altro celano dei rischi, tra questi la possibilità che qualcuno se ne appropri indebitamente.

Utilizza i social network e similari con attenzione e responsabilità. In particolare:

- imposta le opzioni per la privacy nel modo corretto;
- fai attenzione ai link ricevuti nei messaggi o nelle chat da parte di altri utenti: non sempre questi contenuti sono autentici!
- diffida di quegli applicativi che richiedono l'autorizzazione ad accedere ai tuoi dati personali e alla lista dei tuoi indirizzi e-mail;
- digita l'indirizzo del social network direttamente dal tuo browser o usa l'impostazione "preferiti" per evitare il phishing;
- ricorda che tutto ciò che viene pubblicato in un social network potrebbe rimanere per sempre su Internet, anche dopo la cancellazione del tuo profilo;
- il mondo online è reale quanto lo è il mondo offline e su di esso valgono le stesse regole di rispetto e educazione. Comportati bene e richiedi che gli altri facciano altrettanto;

- Casella di posta elettronica: qualche attenzione in più

1) difendersi da Spam – E-mail Bombing

Lo spam consiste nell'utilizzo illecito di sistemi di messaggistica elettronica per l'invio indiscriminato di messaggi non richiesti dall'utente che li riceve.

Di solito si tratta di e-mail commerciali e spesso pubblicizzano servizi e prodotti illegali. Altre volte, invece, sono utilizzate per veicolare truffe attraverso attività di phishing.

Per proteggersi dallo spam è consigliabile:

- utilizzare le impostazioni di sicurezza della tua casella di posta per segnalare e mettere in "quarantena" le e-mail di spam;
- leggere prima di selezionare o deselezionare le opzioni relative all'invio di materiale pubblicitario o altre tipologie di aggiornamento

e verificare l'utilizzo delle tue informazioni su termini e condizioni del servizio;
- Per non confermare la correttezza e l'esistenza del tuo indirizzo e-mail: non rispondere mai allo spam e stai attento ai link che promettono di "cancellarti" a meno che non conosca il sito: gli spammer usano spesso questi metodi per essere certi che la casella di posta sia ancora attiva. Non causerebbero quindi una cancellazione ma uno spam maggiore.

2) sicurezza degli allegati

Gli allegati alle e-mail sono diventati uno strumento pratico ed efficiente per ricevere e inviare documenti. Purtroppo, però, essi sono spesso usati per veicolare malware.

Per tale motivo è consigliabile:
- usare molta cautela quando si aprono gli allegati, anche se sembrano provenire da una persona conosciuta. Se è possibile, contatta con altri mezzi coloro che hanno inviato l'allegato prima di aprirlo, la stessa cautela va usata per tutte quelle e-mail che sembrano provenire dal tuo ISP o da società di software che dicono di avere in allegato patch o software antivirus, poiché gli ISP e le società non inviano patch o software via e-mail;
- non aprire gli allegati provenienti da indirizzi e-mail sconosciuti;
- effettuare sempre una scansione prima di aprire gli allegati, almeno per quelli provenienti da persone sconosciute.