

Ritorniamo sull'argomento della difesa dai rischi informatici, un tema ancora più attuale dopo mesi di lavoro a distanza dovuto alle misure di contrasto alla pandemia di Covid-19. Tutti noi, utilizzando strumenti elettronici ed informatici, dobbiamo diventare "ciberconsapevoli", cioè evitare rischi e truffe informatiche mantenendo il pieno controllo dei nostri strumenti e delle nostre azioni. Ecco le principali modalità con cui possiamo venire attaccati da malintenzionati:

PHISHING


CHE COS'E'?

È come pescare, ma il pesce sei tu. Gli attaccanti usano le e-mail come esca per indurti a cliccare link e ad aprire allegati che installano dei programmi dannosi.

RICORDA

Sii CERTO prima di aprire o cliccare. Nel dubbio, chiedi a qualche esperto di controllare il collegamento o l'allegato.

COME SCOPRILO?

-  Sembra urgente
-  Sembra ufficiale (controlla l'indirizzo mittente)
-  Il messaggio inizia e/o finisce con dei saluti generici
-  Il messaggio chiede informazioni personali
-  Formato e aspetto non sembrano corretti

ESEMPI

"Cura per il Covid-19"

"Nuova fattura emessa a tuo carico"

VISHING






CHE COS'E'?

È come il phishing ma gli attaccanti cercano di convincerti a fornire informazioni personali per telefono.

RICORDA

Non fornire informazioni lavorative o personali se non sei sicuro di chi c'è all'altro capo della linea.

COME SCOPRILO?

-  Non hai mai parlato con questa persona
-  Sei stato chiamato, non lo hai fatto tu
-  Vogliono una risposta immediatamente
-  Sostengono che qualcosa è andato storto e che la loro richiesta è assolutamente normale
-  Sostengono di essere tuoi colleghi o dipendenti della banca, di un cliente o di un fornitore

"Urgente: modifica le tue credenziali di accesso"

"Combatti il Coronavirus"

SMISHING





CHE COS'E'?

È come il phishing ma fatto usando i messaggi SMS.

RICORDA

Non fare click sui collegamenti negli SMS (e non rispondere nemmeno).

COME SCOPRILO?

-  Non hai mai ricevuto SMS da questo numero
-  Non riconosci il numero (se viene mostrato)
-  Si presenta come qualcuno che conosci (ad esempio Poste Italiane)
-  Contiene un link e ti chiede di usarlo

"Organizzazione Mondiale della Sanità (OMS): Allarme virus"

In questa lotta il nostro ruolo è un po' quello del "firewall umano". Di seguito un elenco di cose da fare e non fare:

Il Phishing e le sue varianti fanno parte di un insieme più grande di attacchi definiti di "ingegneria sociale". Apparati hardware e programmi di controllo non possono proteggere completamente da questo tipo di attacchi perché questi inducono le persone a compiere azioni contrarie ad una buona politica di sicurezza informatica!

FARE

E

NON FARE

COSA FARE

- ✘ Cambia **regolarmente** le password
- ✘ Usa **password forti** su tutti i dispositivi mobili
- ✘ Mantieni **aggiornati** browser e antivirus
- ✘ Controlla i **casi sospetti** con una seconda fonte di informazioni
- ✘ Controlla **tutti i collegamenti Internet**
- ✘ Riferisci **subito** i problemi ai tuoi responsabili della sicurezza
- ✘ Educa **te stesso e chi lavora con te**
- ✘ Sii sempre **diffidente e attento** nel lavoro informatico

COSA NON FARE

- ✘ **Riutilizzare** le password o usare password **banali**
- ✘ Dare volontariamente **informazioni** a sconosciuti
- ✘ Cliccare su **allegati e collegamenti** di e-mail e di messaggi non richiesti
- ✘ Disabilitare le **cifrature** nei dispositivi mobili
- ✘ **Inserire** chiavette Usb sconosciute nel proprio computer
- ✘ **Sentirsi in colpa** a segnalare subito eventuali problemi
- ✘ Pensare di non essere un possibile obiettivo di **attacchi informatici**

SEGUI SUBITO QUESTE INDICAZIONI SE:

- Sei stato soggetto ad un attacco di ingegneria sociale
- Pensi di essere stato infettato da malware
- Pensi che ci possa essere stata divulgazione di informazioni riservate

INDICAZIONI:

- Smetti di usare il computer e spegnilo subito
- Avvisa i responsabili informatici dell'azienda
- Inoltra eventuali documenti o link sospetti ad un indirizzo noto di assistenza informatica
- Richiedi ulteriori istruzioni

Gli attacchi descritti possono capitare a chiunque: non esitare a dare l'allarme il prima possibile, anche se temi di aver commesso un errore. Più la reazione è veloce, minore sarà il possibile danno.