#AprenemCiberseguretat

PHISHING

Què és? TÈCNICA EN LA QUAL ALGÚ SUPLANTA A UNA ENTITAT/SERVEI MITJANÇANT UN CORREU ELECTRÒNIC, SMS O MISSATGE INSTANTANI PER ACONSEGUIR INFORMACIÓ PERSONAL O CONFIDENCIAL D'UN USUARI O USUÀRIA.

Quins mètodes d'atac existeixen?

Fitxers executables
Fan creure a la persona receptora que el fitxer adjunt al correu és legítim assignant-hi una icona representativa de determinat programari com PDF. També pot remetre a un URL i, en fer-hi clic, es descarrega el fitxer.

Fitxers ofimàtics
Inclouen macros en un document que fan referència a un codi embegut en aquest fitxer per a executar una acció nociva. Solen descarregar i executar un programa que permet el control remot de la màquina.

Usurpació remitent
Suplanta el compte i el domini real del remitent. Per a poder suplantar el domini d'un usuari, el servidor DNS que hi està associat ha de mancar d'unes certes mesures de seguretat.

Ús del caràcter RLO
S'aprofita de determinats caràcters Unicode per representar unes certes cadenes de manera inversa. Exemple: “FACTURA2023_xcod.exe” es converteix en “FACTURA2023_exe.docx”.

Enllaços nocius
S'utilitzen enllaços nocius per executar codi en l'equip de la víctima o obtindre’n informació.

Ocultar extensió
Per a ocultar l'extensió s'afigen espais just abans de la vertadera extensió del fitxer nociu amb l'objectiu que no es puga visualitzar. Eixe espai es mostra com a tres punts (…).

BONES PRÀCTIQUES

1. **NO OBRIU CAP ENLLAÇ NI DESCARREGUEU CAP FITXER** adjunt procedent d'un correu electrònic/SMS/missatge que presente qualsevol indici o patró fora de l'habitual.
2. **NO CONFIEU ÚNICAMENT EN EL NOM DE LA PERSONA REMITENT.** Comproveu que el domini del correu rebut és de confiança. Si un correu procedent d'un contacte conegut sol·licita informació inusual, contacteu amb ell o ella per un altre mitjà per a verificar-ho. També podeu buscar el domini del correu en algun motor de cerca al costat de paraules com *phishing*, programari maliciós o frau**.**
3. Abans d'obrir qualsevol fitxer descarregat des del correu, **ASSEGUREU-VOS-EN DE L'EXTENSIÓ** i no us fieu de la icona associada a aquest.
4. **NO HABILITEU MACROS** dels documents ofimàtics, encara que el mateix fitxer ho sol·licite**.**
5. **NO FEU CLIC EN CAP ENLLAÇ** que sol·licite dades personals o bancàries.
6. Tingueu **ACTUALITZAT EL SISTEMA OPERATIU**, aplicacions ofimàtiques i navegador.
7. Utilitzeu **EINES DE SEGURETAT COMPLEMENTÀRIES** al programari antivirus per a mitigar atacs.
8. **EVITEU FER CLIC** directament en qualsevol enllaç des del mateix client de correu. Si l'enllaç és desconegut, és recomanable buscar informació en els motors de cerca.
9. **UTILITZEU CONTRASENYES ROBUSTES** per a accedir al correu electrònic. Renoveu-les periòdicament. Empreu doble autenticació si és possible.
10. **XIFREU MISSATGES DE CORREU** que continguen informació sensible.

WWW.UV.ES/UVSTIC

VNIVERSITAT DE VALÈNCIA UVSTIC
Vicerectorat d'Estratègia, Qualitat i Tecnologies de la informació
Conscienciació en la seguretat de la informació