FRAUDA ”MESAJ DE LA ȘEF”

Frauda ”Mesaj de la șef” vizează angajații autorizați să efectueze plăți, care, prin inducere în eroare, sunt determinați să plătească o factură falsă ori să efectueze un transfer.

CUM FUNCȚIONEAZĂ?

Un infractor sună sau trimite un e-mail, pretinzând că este unul din managerii de top din companie.

De obicei este bine informat cu privire la organizație.

Solicită efectuarea urgentă a unei plăți.

Folosește un limbaj persuasiv, de tipul: ”avem încredere în tine, rămâne între noi, eu sunt ocupat acum”.



Se referă la o situație sensibilă (ex. control autorități, achiziții etc.).

Angajatului i se cere să nu respecte procedura obișnuită de autorizare a plăților.

Instrucțiuni complete pot fi trimise mai târziu, de către o persoană sau prin e-mail.

Angajatul transferă banii într-un cont al atacatorului.

Deseori, solicită ca plata să se facă într-un cont din afara țării și chiar a Europei.

CARE SUNT SEMNELE?

- E-mail sau apel telefonic nesolicitat.
- Contact cu un angajat, de regulă din conducere, cu care nu ești în legătură. directă, în mod normal.
- Solicitare de confidențialitate.
- Presiune sub semnul presupusei urgențe.
- Solicitare neobișnuită, ieșită din tiparele procedurilor interne.
- Amenințări sau promisiuni neobișnuite, flatare.

CE POȚI FACE?

CA ORGANIZAȚIE

Conștientizați riscul și asigurați-vă că **angajații sunt informați permanent**.

Instruiți-vă staff-ul să manifeste **atenție maximă la efectuarea plăților**.

Implementați proceduri interne stricte referitoare la plăți.

Implementați proceduri de verificare a legitimității plăților solicitate prin e-mail.

Stabiliți reguli de raportare a tentativelor de fraudă.

Verificați datele publicate pe site-ul companiei, **restricționați accesul la datele importante** și fiți atenți la rețelele sociale.

Actualizați soluțiile tehnice de securitate.

Sesizați poliția la orice încercare de fraudă, chiar dacă nu ați devenit victima acesteia.

CA ANGAJAT

Respectați cu strictețe procedurile de securitate în cazul plăților și achizițiilor. **Nu săriți nici un pas procedural și rezistați presiunilor.**

Verificați cu atenție adresele de e-mail când primiți solicitări de informații sensibile/transferuri de bani.

Dacă aveți dubii în cazul unui transfer de bani, **consultați un coleg.**

Niciodată nu deschideți link-uri sau atașamente dubioase primite prin e-mail. Fiți foarte atenți când verificați mail-ul personal pe calculatorul de serviciu.

Manifestați precauție și restricționați informațiile de pe rețelele sociale.

Evitați publicarea de date despre conducerea, securitatea sau procedurile firmei.

Dacă primiți un e-mail suspect, informați imediat departamentul IT.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ - CERT-RO

#CyberScams