FRAUDA ”MESAJ DE LA ȘEF”

Frauda ”Mesaj de la șef” vizează angajaţii autorizaţi să efectueze plăţi, care, prin inducere în eroare, sunt determinaţi să plătească o factură falsă ori să efectueze un transfer.

CUM FUNCȚIONEAZĂ?

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

De obicei este bine informat cu privire la organizaţie.

Solicită efectuarea urgentă a unei plăţi.

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

Se referă la o situaţie sensibilă (ex. control autorităţi, achiziţii etc.).

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

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

Angajatul transferă banii într-un cont al autorului.

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

CARE SUNT SEMNELE?

- E-mail sau apel telefonic nesolicitat.
- Contact cu un oficial cu care nu ești în legătură directă, în mod normal.
- Solicitare de confidenţialitate.
- Presiune sub semnul presupusei urgenţe.
- Solicitare neobișnuită, ieșită din tiparele procedurilor interne.
- Ameninţări sau promisiuni neobișnuite, flatare.

CE POȚI FACE?

CA ORGANIZAŢIE

Conștientizaţi riscul și asiguraţi-vă că **angajaţii sunt informaţi permanent**.

Instruiţi-vă staff-ul să manifeste **atenţie maximă la efectuarea plăţilor**.

Implementaţi proceduri interne stricte referitoare la plăţi.

Implementaţi proceduri de verificare a legitimităţii plăţilor solicitate prin e-mail.

Stabiliţi reguli de raportare a tentativelor de fraudă.

Verificaţi datele publicate pe site-ul companiei, **restricţionaţi accesul la datele importante** și fiţi atenţi la reţelele sociale.

Actualizaţi soluţiile tehnice de securitate.

Sesizaţi poliţia la orice încercare de fraudă, chiar dacă nu aţi devenit victima acesteia.

CA ANGAJAT

Respectaţi cu strictețe procedurile de securitate în cazul plăţilor și achiziţiilor. **Nu săriţi nici un pas procedural și rezistaţi presiunilor.**

Verificaţi cu atenţie adresele de e-mail când primiţi solicitări de informaţii sensibile/transferuri de bani.

Dacă aveţi dubii în cazul unui transfer de bani, **consultaţi un coleg.**

Niciodată nu deschideţi link-uri sau atașamente dubioase primite prin e-mail. Fiţi foarte atenţi când verificaţi mail-ul personal pe calculatorul de serviciu.

Manifestaţi precauţie și restricţionaţi informaţiile de pe reţelele sociale.

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

Dacă primiţi un e-mail suspect, informaţi imediat departamentul IT.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLIȚIA ROMÂNĂ

#CyberScams