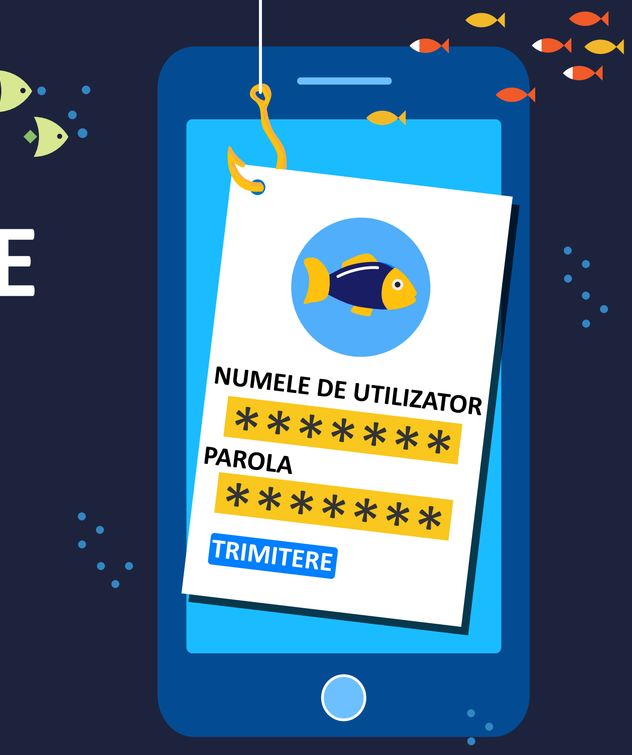
AMENINŢĂRI PE WEB

VERIFICAŢI DE DOUĂ ORI ÎNAINTE DE A FACE CLIC.

Vă puteţi pierde banii, informaţiile personale şi chiar datele stocate, dacă dispozitivul încetează să mai funcţioneze. Nu vă lăsaţi înşelat!



CUM S-AR PUTEA ÎNTÂMPLA ACEST LUCRU?

ATACURILE PHISHING: Acestea păcălesc utilizatorii să ofere informaţii personale asumându-şi calitatea de instituţie de încredere. Acestea se transmit prin e-mail, mesaje text sau platforme ale reţelelor de socializare.

NAVIGAREA PE WEB: Dispozitivul dvs. mobil poate fi infectat accesând pur şi simplu o pagină web nesigură.

DESCĂRCAREA FIŞIERELOR: Linkurile şi anexele rău intenţionate pot fi incluse direct într-un e-mail.

DE CE ESTE EFICIENT?

Dispozitivele mobile sunt **CONECTATE ÎN PERMANENŢĂ** la internet.

DIMENSIUNEA REDUSĂ A ECRANULUI DISPOZITIVULUI este o constrângere generală. Browser-ele mobile afişează adrese URL într-un spaţiu limitat al ecranului, fiind astfel dificil să vedeţi dacă domeniul este legitim.

ÎNCREDEREA IMPLICITĂ A UTILIZATORULUI în natura personală a unui dispozitiv mobil.

CE PUTEŢI FACE?

Fiţi suspicios dacă primiţi un SMS sau un apel telefonic de la o companie care vă solicită informaţii personale. Puteţi verifica dacă mesajul/apelul este legitim prin apelarea directă a companiei la numărul lor oficial.

https://

Atunci când navigaţi pe web de pe dispozitivul dvs. mobil, asiguraţi-vă că această conexiune este securizată prin HTTPS. Puteţi verifica întotdeauna acest lucru la începutul adresei URL.

Nu faceţi niciodată clic pe un link/o anexă dintr-un e-mail sau SMS nesolicitat. Ştergeţi-l imediat.

^BE:%}
W@RY
*)Z#$=

Aveţi grijă dacă accesaţi o pagină web care conţine greşeli gramaticale, greşeli de ortografie sau cu rezoluţie mică.

Dacă este disponibilă, instalaţi o aplicaţie de securitate mobilă care vă va avertiza în cazul oricărei activităţi suspicioase.

EUROPOL EC3 European Cybercrime Centre | POLIŢIA ROMÂNĂ | DIICOT | CERT.RO | #MobileMalware