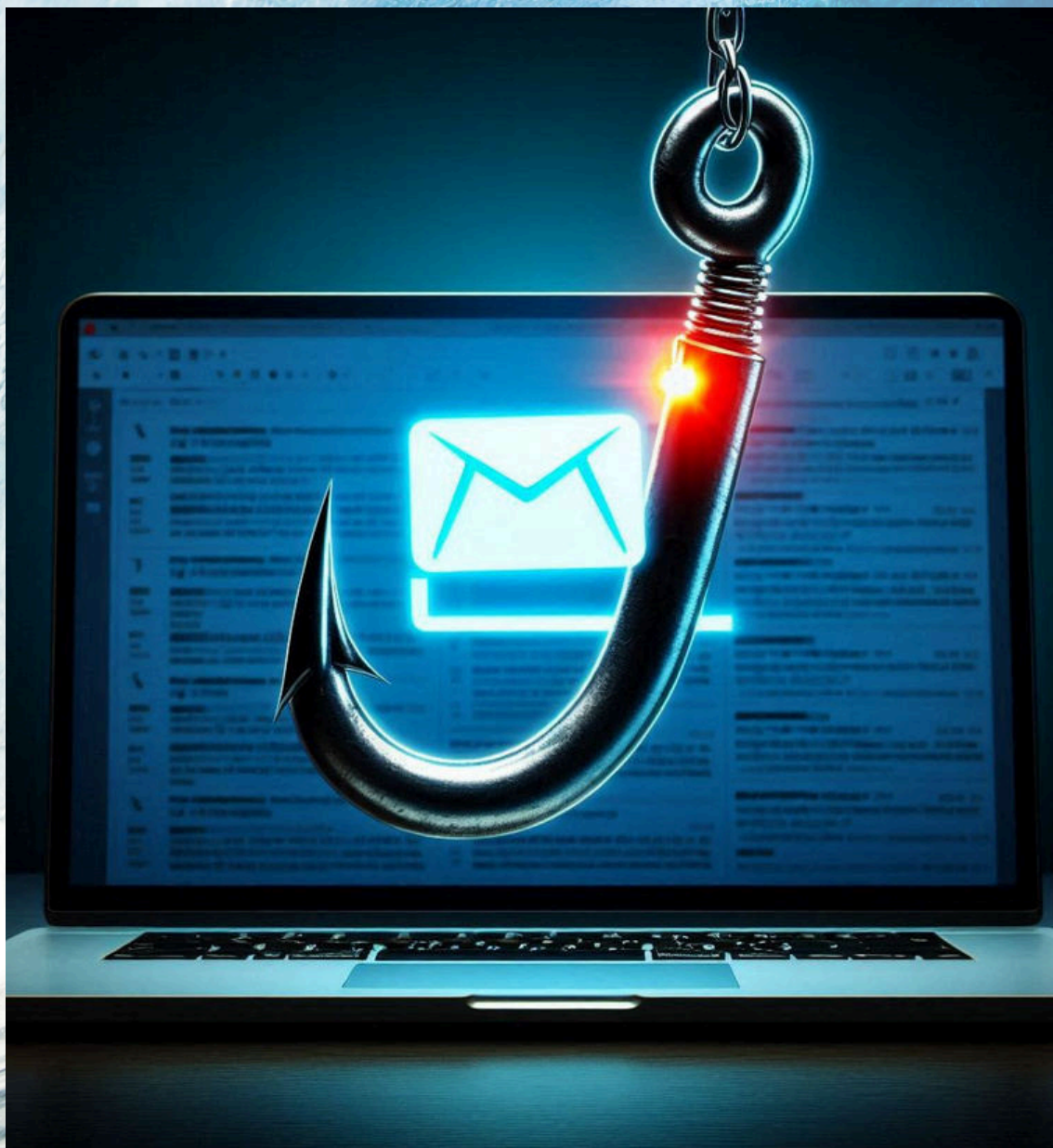


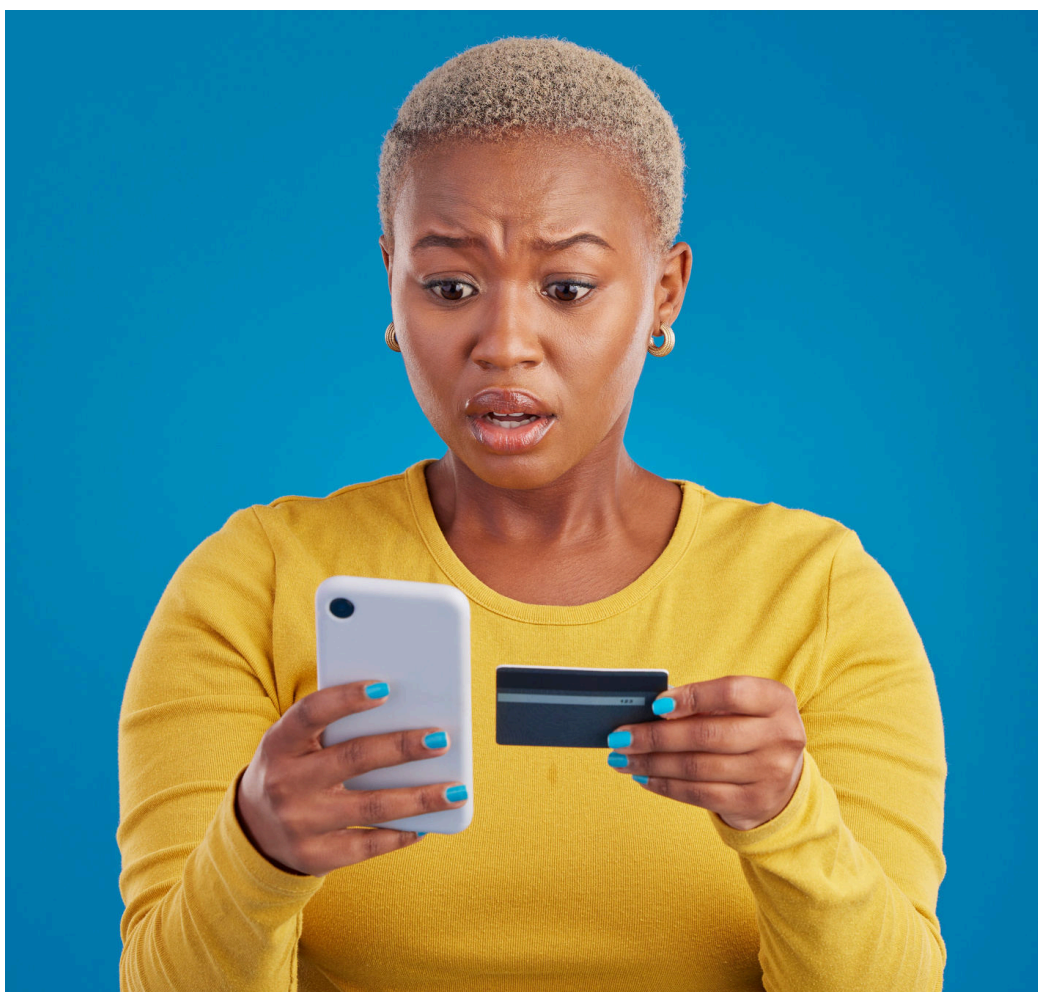
NAVIGHEAZĂ ÎN SIGURANȚĂ PE APELE TULBURI ALE ESCROCHERIILOR DE PE INTERNET



www.safewiz.eu



CE ESTE PHISHINGUL?



Phishingul este o metodă de atac cibernetic. Numele vine din cuvântul englezesc „fishing” (pescuit), pentru că atacatorii „pescuiesc” informații sensibile aruncând o momeală atrăgătoare.

Acești escroci se dau adesea drept cineva cunoscut, cum ar fi banca ta sau un magazin online popular, ca să te convingă să le dai date personale: parola, datele cardului sau datele de autentificare. Pot pretinde că există o problemă urgentă, cum ar fi o problemă de securitate sau un cont blocat, ori o ofertă incredibilă, ca să pară că trebuie să acționezi imediat.

Citeste mai multe pe [blog](#)



TEHNICI COMUNE DE PHISHING



SMISHING - PHISHING PRIN SMS

Phishing prin mesaje text: atacatorii trimit linkuri către site-uri malițioase sau te îndeamnă să suni la numere frauduloase, ca să-ți fure datele sau să-ți instaleze malware.

PHISHING PRIN EMAIL

Emailuri false, care par trimise de bănci sau colegi, te îndeamnă să dezvălui date personale sau să dai clic pe linkuri malițioase.



SITE-URI CLONATE

Atacatorii creează copii fidele ale unor emailuri sau site-uri legitime, ușor modificate ca să conțină linkuri sau atașamente malițioase, astfel încât victimele să le creadă autentice. Datele de autentificare sau de plată pe care le introduci ajung direct la atacatori.



TEHNICI COMUNE DE PHISHING



SPEAR PHISHING (PHISHING ȚINTIT)

Atacuri foarte bine țintite: atacatorii adună informații despre victimă ca să creeze mesaje personalizate și convingătoare, cu șanse mai mari de reușită.

MANIPULARE PE REȚELELE SOCIALE

Atacatorii manipulează sau se dau drept alte persoane pe rețelele sociale, ca să obțină informații personale sau sensibile. Se pot prezenta ca echipa de suport a platformei, prieteni, colegi sau influenceri, ca să-ți câștige încrederea înainte să-ți ceară date sau bani.



VISHING - PHISHING PRIN TELEFON

Escrocii te sună ca să te convingă să le dai informații sensibile sau bani. Persoanele în vârstă sunt cel mai des vizate.



COSTURILE

01

Pierderi financiare

Atacurile de phishing pot provoca pagube financiare mari prin tranzacții frauduloase sau furt de date.

02

Reputație afectată

Companiile lovite de phishing își afectează adesea reputația și pierd încrederea și loialitatea clienților.

03

Scurgeri de date

Datele personale sau ale firmei compromise prin phishing pot duce la scurgeri de date pe scară largă și la folosirea lor abuzivă.

04

Sanțiuni legale

Organizațiile care nu protejează datele clienților pot primi amenzi sau pot fi date în judecată după un incident de phishing.

05

Întreruperea activității

Phishingul poate opri sistemele și poate întrerupe serviciile și productivitatea cât timp firma se recuperează după atac.

06

Furt de identitate

Victimele phishingului riscă furtul identității: atacatorii se pot da drept ele pentru activități ilegale.



6 LUCRURI DE REȚINUT CA SĂ PREVII PHISHINGUL

Cum previi phishingul prin email

Folosește filtre de email ca să blochezi mesajele suspecte și activează autentificarea multi-factor (MFA). Învăță să recunoști tacticile escrocilor și verifică mereu expeditorul înainte să dai clic pe linkuri sau să descarci atașamente. Dacă bănuiești o înșelătorie bancară, contactează direct banca să confirmi mesajul.

Cum nu cazi în capcana site-urilor clonate

Instalează extensii anti-phishing și actualizează periodic setările de securitate ale browserului. Reține: ca să primești bani nu trebuie să introduci niciodată datele cardului, așa că nu le trimite prin linkuri suspecte. Înainte să introduci datele de autentificare, verifică adresa site-ului cu un instrument ca www.urlvoid.com

Cum previi smishingul și vishingul

Verifică orice cerere sunând direct la numărul oficial al instituției sau la ruda respectivă. Nu da informații personale decât dacă tu ai inițiat contactul. Folosește aplicații de blocare a apelurilor și nu răspunde la numere necunoscute. Nu da date sensibile la telefon; contactează firmele doar prin numere sau site-uri verificate. Blochează imediat numerele suspecte.



6 LUCRURI DE REȚINUT CA SĂ PREVII PHISHINGUL

Cum previi phishingul când vinzi online

Când publici un anunț de vânzare, nu muta conversația în afara platformei. Folosește doar mesageria oficială și nu da date personale prin alte canale. Verifică identitatea cumpărătorilor și ai grijă la ofertele prea bune ca să fie adevărate. Raportează imediat mesajele suspecte.

Protecția datelor e cel mai bun aliat al tău

Confidențialitatea datelor e esențială în lumea digitală de azi. Când îți protejezi informațiile personale, previi furtul de identitate, pierderile financiare și accesul neautorizat la conturile tale, iar datele sensibile rămân private și în siguranță. Folosește parole unice și puternice și un manager de parole.

Raportează tentativele de phishing

Dacă bănuiești o tentativă de phishing, raporteaz-o departamentului IT al organizației tale sau unei platforme de securitate cibernetică, ca să-i ajuți pe alții să nu devină victime.



Fii cu un pas înaintea escrocului virtual

Informarea și instrumentele potrivite sunt esențiale în apărarea împotriva atacurilor de phishing.

Dacă te informezi constant și folosești soluțiile recomandate, îți reduci semnificativ riscul de a cădea în capcana phishingului. Fii mereu atent la semnale și păstrează-ți mediul digital în siguranță.

Cine sunt?

Sunt Brîndușa, Senior Software Test Analyst – specialist în testare software. De-a lungul anilor am oprit mii de bug-uri înainte să ajungă în producție. Aduc în fiecare proiect 15 ani de atenție la detalii și o gândire centrată pe utilizator.

În timpul liber îmi place să călătoresc în locuri pline de istorie și cu mâncare excelentă. Pasiunea pentru culturi și bucătării diferite mă ajută să privesc munca dintr-o perspectivă nouă și să găsesc, cu creativitate și deschidere, chiar și cele mai ascunse defecte.

Mă găsești pe **LinkedIn** și pe **site-ul meu Safewiz**



Multumesc!