Ghid informativ privind prevenirea atacurilor Phishing

INTRODUCERE

Atacurile de tip „phishing” reprezintă una dintre cele mai comune și periculoase metode de fraudă cibernetică utilizate pentru a fura informații personale și financiare. Denumirea „phishing” provine de la cuvântul englezesc „fishing”, fiind o analogie pentru „pescuitul” de informații de la victime neavizate.

Ce este phishingul?

Escrocii trimit mesaje pentru a determina utilizatorii să acceseze un link sau să deschidă un atașament care le oferă posibilitate de ați accesa datele personale sau a instala un program malware pe dispozitiv.

Mesajele de tip phishing sunt create într-un mod în care par să provină de la banca, site-ul dvs. de comerț electronic, universitate, guvern, angajator, rude sau colegi. Ele pot conține atașamente încărcate cu programe malware, linkuri rău intenționate sau redirecționări către site-uri web spam.

Tipuri de phishing

- **Email Phishing:** Cel mai comun tip de atac, în care atacatorii trimit e-mailuri frauduloase care par să provină de la organizații legitime. Aceste e-mailuri conțin de obicei un link către un site fals care imită un site autentic și solicită utilizatorului să introducă informații personale, cum ar fi nume de utilizator, parole. La fel ele pot conține atașamente sau link-uri malițioase.
- **Spear Phishing:** Spre deosebire de atacurile de tip phishing general, spear phishing țintește o persoană sau o organizație specifică. Atacatorii folosesc informații personalizate pentru a face mesajele lor mai convingătoare și mai greu de detectat.
- **Whaling:** Un tip de spear phishing care vizează persoane de rang înalt într-o organizație, cum ar fi directori executivi sau manageri de nivel superior. Atacurile whaling sunt foarte sofisticate și bine documentate pentru a exploata informațiile sensibile ale companiei.
- **Smishing:** Similar cu email phishing, dar utilizând mesaje SMS. Utilizatorii primesc mesaje text care par să provină de la surse de încredere și sunt îndrumați să acceseze linkuri sau să dezvăluie informații personale.
- **Vishing:** Implică apeluri telefonice frauduloase în care atacatorii pretind a fi reprezentanți ai unor organizații legitime și încearcă să obțină informații sensibile direct de la victimă.
- **Phishing pe social media:** Primiți mesage pe platformele de socializare care te vor redecționa, printr-un link, către o platformă asemănătoare celei originale. De asemenea, ai putea primi un mesaj care te informează că există o problemă cu contul tău de social media și că trebuie să te conectezi din nou la el pentru a corecta situația. Pagina pe care vei fi redirecționat îți va cere să introduci userul și parola care vor ajunge pe mâna hackerilor.

Semne ale atacurilor de tip phishing

- **Expeditor necunoscut sau suspicios:** Verifică adresa de e-mail a expeditorului. Deseori, adresele de e-mail folosite de atacatori conțin mici modificări față de adresele legitime (de exemplu, un caracter în plus sau o literă schimbată).
- **Greșeli gramaticale și ortografice:** E-mailurile și mesajele de phishing conțin adesea greșeli gramaticale și ortografice, deoarece sunt redactate rapid sau traduse automat din alte limbi.
- **Urgentarea și presiunea:** Mesajele de phishing încearcă adesea să creeze un sentiment de urgență sau panică. De exemplu, îți pot spune că contul tău va fi suspendat dacă nu acționezi imediat.
- **Linkuri și atașamente suspecte:** Atacatorii includ adesea linkuri care duc către site-uri false. Plasează cursorul peste linkuri pentru a verifica adresa URL reală. Atașamentele suspecte pot conține malware sau programe de tip keylogger.
- **Solicitări neobișnuite de informații personale:** Fii precaut cu mesajele care solicită informații personale sau financiare. Instituțiile legitime nu cer astfel de informații prin e-mail.
- **Informații ambigue** - dacă mesajul primit nu-ți spune foarte multe, dar are un link pe care ești invitat să îl accesezi, ai face bine să eviți asta.

Măsuri de prevenire

- **Utilizarea software-ului de securitate:** Instalarea și actualizarea regulată a software-ului antivirus și anti-malware pe toate dispozitivele folosite.
- **Autentificarea în doi pași:** Activează autentificarea în doi pași pentru conturile tale, adăugând un nivel suplimentar de securitate.
- **Verificarea dublă:** Înainte de a furniza informații personale, contactează direct organizația printr-un număr de telefon sau o adresă de e-mail cunoscută.
- **Crearea unui back up a datelor personale:** În cadrul unui atac phishing datele tale pot fi distruse, modificate sau criptate. Folosește un hard disck extern sau un spațiu de stocare cloud pentru a face o copie de rezervă, de unde vei putea să-ți recuperezi informația în caz de pierdere.
- **Instruirea continuă a personalului**: Educația eficientă în materie de phishing, inclusiv cunoștințe conceptuale și feedback, este o parte importantă a strategiei anti-phishing a oricărei organizații.

Acțiunile în cazul în care ai accesat un link phishing

- **Deconectează dispozitivul de la internet:** Aceasta va reduce riscul de răspândire a programelor malware și poate preveni conectatea la dispozitivul dumneavoastră din exterior.
- **Scanează dispozitivul cu un antivirus:** Un antivirus actulizat la zi poate depista programele malware instalate pe dispozitiv.
- **Schimbă toate parolele** - intră pe toate platformele care știi că ar putea avea legătură cu cea de pe care ai accesat linkul și schimbă parolele.
- **Blochează conturile bancare** - dacă ai completat undeva datele cardului tău, sună rapid la bancă și blochează contul despre care e vorba.

Pentru a raporta orice incidente de securitate cibernetică, vă rugăm să vizitați **cyberevent.gov.md** sau să ne contactați la : **info.cert@stisc.gov.md**