PHISHING

Phishing është një formë e inxhinierisë sociale në të cilën një aktor keqdashës paraqitet si një burim legjitim, si një koleg, i njohuri juaj ose organizatë e besueshme, për të joshur një viktimë me qëllim marrjen e informacioneve sensitive ose akses në rrjet. Sulmi mund të jetë në formën e një emaili, mesazhi tekst, apo edhe një telefonate.

Nëse është e suksesshme, kjo teknikë mund t'u mundësojë aktorëve keqdashës të kenë akses fillestar në një rrjet dhe pasojat e sulmit të prekin organizatën e synuar dhe palët e treta të lidhura me të. Rezultati i këtij sulmi mund të jetë humbje e të dhënave ose shërbimit, vjedhje e identitetit, infeksion malware ose ransomware.

Kujdes! Mos bini viktimë e sulmeve Phishing!

Ju mund të parandaloni suksesin e sulmeve phishing dhe të kufizoni ndikimet e tij negative.

Ja se si funksionon një sulm phishing:

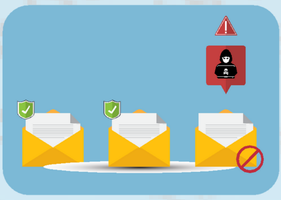
1 ZGJEDHJA E "KARREMIT"

Karremi zakonisht përbëhet nga një email me një përmbajtje subjekti që e josh përdoruesin të hapë emailin, p.sh., subjekti përmban një sinjalizim, një veprim ose kërkesë për informacion. Disa subjekte të përdorura nga fushata të suksesshme phishing janë:

- Njoftim i rëndësishëm nga banka
- Njoftime brenda organizatës
- Njoftime specifike për përdoruesit, si mundësi trajnimi

2 HEDHJA E GREPIT

Aktorët e sulmeve phishing hedhin "grepa" të shumtë për të rritur mundësinë e tyre për sukses dhe më pas presin që një viktimë të kapë "karremin".



3 KAPJA E VIKTIMËS

Aktori keqdashës ka një sulm të suksesshëm kur një email nuk bllokohet nga masat mbrojtëse të rrjetit dhe arrihet që një viktimë t'i përgjigjet me informacione të vlefshme ose ekzekuton një dokument të infektuar që gjendet në *attachment*. Aktori keqdashës më pas mund të zotërojë informacione të ndjeshme, kredenciale ose atribute të tjera për të kompromentuar përdoruesit nëpërmjet malware.

PARANDALONI SULMET PHISHING

1 BLLOKO

- Implementoni masa mbrojtëse për rrjetin dhe pajisjet tuaja - si një barrierë fillestare për të reduktuar mundësinë për një përpjekje të suksesshme phishing
- Konfiguroni serverët e postës elektronike për të përdorur protokollet që verifikojnë legjitimitetin e komunikimeve me email, si Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), dhe Domain-Based Message Authentication, Reporting, and Conformance (DMARC).
- Përfshini listat e mohimit (*denylist*) ose burimet e inteligjencës së kërcënimeve kibernetike në rregullat e *Firewall* për të bllokuar domain-e *malicious*, URL dhe adresa IP.

2 EDUKOHU

- Edukohuni për të identifikuar indikatorë të sulmeve phisihing, të tilla si të adresa e dyshimta të postës elektronike të dërguesit, fraza të përgjithshme përshëndetjeje, linqe të dyshimta, emaile me gabime drejtshkrimore ose paraqitjeje dhe bashkëngjitje të dyshimta.
- Mësoni si të qëndroni vigjilentë në të gjitha platformat e komunikimit, duke përfshirë mediat sociale, dhe identifikoni në çdo rast komunikimet e dyshimta.

3 RAPORTO PRANË AKCESK

Nëse merrni një email phishing:

- Raportojeni!
- Mos ua dërgoni miqve apo kolegëve tuaj!