QESTIT

CHECKLISTA

SÅ HÄR GÖR DU FÖR ATT TA REDA PÅ OM DU FÅTT ETT PHISHING-MEJL!

INTRODUKTION

I dagens digitala värld får vi massor av mejl varje vecka från både privatpersoner och företag och det är enkelt att snabbt svara på dem eller göra vad man blir tillsagd. Någon av dessa skulle kunna vara organiserade grupper som försöker skapa sig en väg in i ett företags nätverk. Det kan alltså vara så att avsändaren inte alltid är den som den säger sig vara och det är viktigt att du granskar mejlen innan du agerar.

Cyberattacken Phishing har blivit vanligare och vanligare och fler försöker få tag på värdefull information om dig, så därför har vi gjort en checklista på hur du ska gå tillväga för att ta reda på om du fått ett bluffmejl eller inte.

Vi hoppas att den ska vara till hjälp!

VAD ÄR PHISHING?

Phishing är en av de mest populära cyberattackerna där målet för angriparen är att få tag i värdefull information, om exempelvis ditt bankkonto eller dina lösenord. Personen kan även laddar ner en bakdörr till din dator. Ett Phishing-mejl ser exakt ut som ett autentiskt mejl vid första anblick och därför är det viktigt att vara uppmärksam. Angriparen kommer troligtvis att be dig klicka på en länk, en bilaga eller på något sätt få dig att lämna viktig information.

Det finns även andra sorter av Phishing:

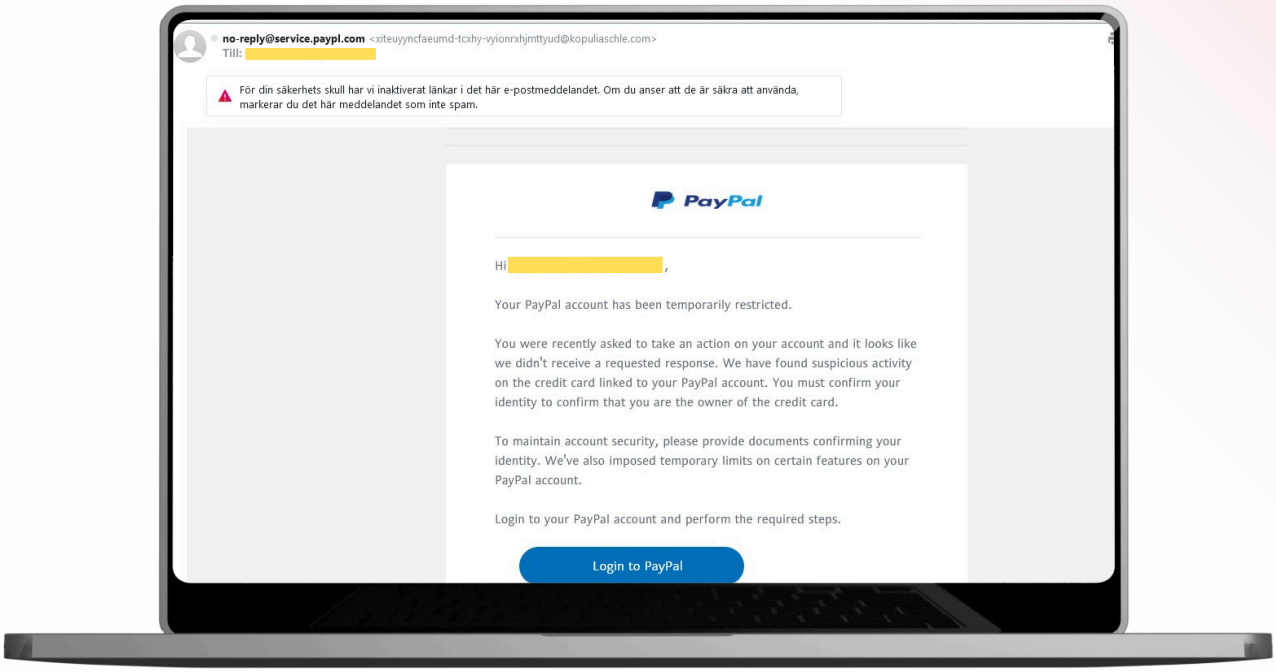
- **Spear Phishing**
  Denna attack går till på samma sätt som en phishing-attack, men skillnaden är att det finns ett specifik mål. Här vet angriparen vem målet är och har information om målet.
- **Vishing**
  Vid denna attack kontaktas målet via telefon istället för mejl.

GRANSKA ANVÄNDAREN

Det är viktigt att granska avsändarens mejladress. Nedan ser du ett mejl som vid första anblicken ser ut att komma från Paypal med mejladressen **no-reply@paypl.com** vilket gör att målet ”i detta fall jag” tror att mejlet kommer från PayPal, men kollar du en extra gång ser du att adressen inte innehåller hela ordet PayPal.

Du kan också se att avsändarens ”angriparens” riktiga mejldress är **xiteuyyncfaeumd-tcxhy-vyionrxhjmttyud@kopuliaschle.com**. Detta visar att mejlet inte kommer från det riktiga företaget Paypal och du bör inte svara eller trycka vidare på någon länk. Ta bort mejlet.

Alla Phishing-mejl är inte lika lätta att syna som detta exemplet och därför är det viktigt att granska avsändaren innan du gör något.



GRANSKA SPRÅKET

Det är också viktigt att reflektera över språket i mejlet.

- **Hur tilltalas du?**
- **Vad handlar mejlet om?**
- **Vad vill avsändaren att du ska göra?**

I bildexemplet ovan blir jag adresserad som min mejladress istället för mitt namn, ett mejl från ett riktigt företag skulle skrivit mitt förnamn och efternamn alternativt bara förnamnet.

Om mejlet ser ut att komma från ett företag eller person som du haft kontakt med innan gäller det att granska språket och se om det är som det brukar vara eller om det är något som sticker ut.

LÄNKAR OCH BILAGOR

Klicka inte på länkar eller bilagor om du inte är säker på vem avsändaren är. När du klickar på en länk i ett Phishing-mejl finns risken att det kommer köras ett script som gör att det installeras en bakdörr till din dator, eller så leds du vidare till en hemsida som ser ut som en ”riktig” hemsida. Väl inne på hemsidan kommer angriparen försöka få dig att lämna lösenord eller uppgifter om ditt bankkonto.

Det finns flertalet publika sidor och tjänster på internet där du kan ta reda på om ditt konto och lösenord förekommer i olika databasdumpar. Exempelvis **https://haveibeenpwned.com/** och **https://www.dehashed.com/**.

HUR DU KAN GÅ TILLVÄGA OM DU MOTTAR ETT PHISHING-MEJL

Om du tror att du mottagit ett phishing-mejl rekommenderar jag att endast skicka det internt till en grupp eller person som hanterar säkerheten på ditt företag. Du kan även varna dina kollegor men tänk på att inte vidarebefordra mejlet.

Om du inte har en grupp eller person som hanterar säkerheten på ditt företag kan du:

- Skicka mejlet till: **phishing-report@us-cert.gov**. Mejlet går då till Security Agency som tillhör USA:s regering där målet är att stoppa Phishing-attacker.

- Skicka länken (URL:en) i ditt mejl till Google via denna länk: **https://safebrowsing.google.com/safebrowsing/report_phish/?hl=enS**. För att inte behöva klicka på knappen/länken i ditt mejl kan du högerklicka för att kopiera länkadressen.

När din rapport är inskickad kommer Google analysera hemsidan och blockera den om det är en bluff. Genom att rapportera när du tror att du fått ett Phishing-mejl hjälper du andra att inte bli lurade.

Vi hjälper företag att prioritera, planera och designa sitt kvalitetssäkringsarbete med expertkompetens inom test, prestanda, automatisering, säkerhet, ledning, kravhantering och UX-design.

info@qestit.se

08-501 108 90

Wallingatan 2 - 111 60 Stockholm

QESTIT

qestit.com