Phishing

Vad är det och hur skyddar du dig?

I Sverige uppger 85 procent av företagen i en undersökning att de under 2020 haft en ökning av cyberattacker*. Hur stor risk är det att du låter dig luras?

Phishing, smishing, spear phishing eller spam?

Kärt barn har många namn? Inte i detta fall. Dessa är benämningar på olika sätt cyberkriminella begår bedrägerier. Phishing, eller nätfiske som det kallas på svenska, är ett bedrägeri där bedragaren försöker lura dig genom att skicka e-postmeddelanden eller SMS (smishing) till dig. Syftet är att lura till sig personlig information som till exempel dina inloggningsuppgifter, e-postadress, lösenord eller bankkortsnummer.

Om angriparen lyckas lura dig till att ladda ner en fil så kan det innebära att du nu omedvetet installerat ett så kallat malware eller ransomware. Det kan i värsta fall resultera i att samtliga filer på din dator och företagets servrar blir krypterade utan möjlighet för någon att använda filerna.

Som du säkert förstår är det hög tid att ta er IT-säkerhet på allvar. I stället för att lösa katastrofen – förebygg den!

IT-Tjänster

Vi är specialister inom IT och tillgodoser era behov och gör er vardag enklare. PrimeQ levererar IT-drift-, support, moln- och konsulttjänster. Vi vet hur viktigt det är att IT-lösningarna fungerar för att verksamheten ska flyta på och vi lägger stor vikt vid personlig service och tar fram system som är noggrant anpassade utefter era behov.

Vill du veta mer om våra IT-tjänster eller PrimeQ?

Vänligen kontakta:
sales@primeq.se

*Källa: Radar, Svensk Cybersäkerhet 2021

Ver. 2021 1.0

25 tips på hur du kan skydda dig

1. **Sunt förnuft och kritiskt tänkande.** Verkar det hela logiskt?
2. **Granska noga – speciellt när ett meddelande manar till snabba åtgärder.** Ett knep många bedragare nyttjar är att uppmana till snabba åtgärder för att du inte ska hinna tänka dig för. Så gör det, ta god tid på dig.
3. **Klicka inte på länkar i misstänksamma meddelanden.** Undersök vart länken går genom att hovra (håll muspekaren över länken (utan att klicka) och läs var länken går.
4. **Öppna inte bifogade filer från okända avsändare.** Kontrollera avsändaren och meddelandet en extra gång innan du öppnar filen.
5. **Fyll inte i uppgifter i formulär.** Om du får ett okänt formulär länkat via e-post eller SMS – undvik att fylla i det tills du vet att du kan lita på källan.
6. **Kontrollera avsändaren.** Verkar något fel i avsändaradressen? Då är det troligtvis inte företaget som påstås ligga bakom meddelandet som har skickat det.
7. **Kontrollera stavning och språk.** Utländska bedragare använder sig ofta av program som automatiskt översätter sina meddelanden från sitt språk. Dessa program är inte perfekta vilket ofta leder till syftningsfel eller felstavningar.
8. **Kontakta källan.** Osäker på om det är företaget eller myndigheten som skickat meddelandet till dig? Kontakta dem via telefon eller en officiell e-postadress som du kan hitta via Google eller deras webbplats. Svara inte på meddelandet i din inkorg. **Kom ihåg: Seriösa företag, banker eller myndigheter uppmanar aldrig sina kunder att lämna ut personliga uppgifter via e-post.**
9. **Använd inte samma lösenord till flera tjänster.** Om tjänsten inte har stöd för MFA (multifaktorautentisering) bör du använda unika lösenord, eller ännu bättre - lösenordsfraser till varje tjänst.
10. **Skriv inte ned dina lösenord på en post-it.** Använd en pålitlig lösenordshanterare så att du slipper skriva ner lösenordet på en post-it-lapp under ditt tangentbord. Jo, det händer faktiskt fortfarande!
11. **Svara inte på roliga tester som "Minns du namnet på ditt första husdjur?" på sociala medier.** Känner du igen frågan? Precis – det är samma typ av frågor som vissa molntjänster använder för att återställa ditt lösenord. Ge inte bort personlig information till vem som helst på internet även om det handlar om ett roligt test.
12. **Svara aldrig på ett spam.** Då bekräftar du bara att din e-postadress fungerar och du riskerar att få ännu mer skräppost.

Ver. 2021 1.0

25 tips på hur du kan skydda dig

13. **Ställ in så att ditt e-postprogram inte laddar ner bilder automatiskt.** Även detta kan bekräfta att din e-postadressfungerar. Är du osäker på hur du gör? Kontakta din IT-support
14. **Avregistrera dig inte från suspekta nyhetsbrev.** Ja, du läste faktiskt rätt. Istället för att avregistrera dig och bekräfta din e-postadress eller telefonnummer, välj att spärra avsändaren.
15. **Använd spamfilter.** Det hjälper inte mot all form av spam men hjälper dig att hålla borta en stor del av oönskad e-post.
16. **Uppdatera ditt virusprogram.** Även om antivirusprogram inte upptäcker all skadlig kod så fyller de fortfarande en funktion. Se till att hålla ditt program uppdaterat för att öka möjligheten att stoppa angrepp.
17. **Håll operativsystem, webbläsare och insticksprogram uppdaterade.** Tänker du som många att ”jag gör det sen”? Bedragare utnyttjar gärna kända säkerhetsbrister i både operativsystem och webbläsare men även i insticksprogram som till exempel Java och Adobe Flash. Uppdatera så fort notis om uppdatering finns tillgänglig. Det är värt det!
18. **Se till att ditt företag har konfigurerat autentiseringsmetoderna SPF, DKIM och Dmarc för er domän.** Detta är något du kan fråga din IT-support.
19. **Använd MFA (multifaktorautentisering).** Använd MFA eller passwordless på alla tjänster där det finns stöd för detta.
20. **Använd lösenordsfras istället för ett lösenord.** Som vi nämnde ovan blir det mycket svårare för en bedragare att knäcka ditt lösenord genom att låta automatiserade program pröva olika möjliga kombinationer. Visste du att det dessutom är enklare att komma ihåg en fras än ett lösenord?
21. **Betrakta din personliga information som känslig data.** Dela inte med dig av uppgifter i onödan.
22. **Ta hjälp av betrodda och bra tjänster på internet.** Du hittar några exempellänkar i slutet av denna lista.
23. **Håll dig uppdaterad om aktuella säkerhetshot.** Du hittar några pålitliga källor i slutet av denna lista.
24. **Är du osäker om det är ett phishingmejl eller spam?** Ta det säkra före det osäkra och vidarebefordra mejlet till er servicedesk. Det kanske är fler som anmält samma försök till nätfiske men du kan också vara först och bidra till att stoppa en attack. Servicedesk är specialister på att genomskåda försök till nätfiske och de vill dessutom få information om eventuella attacker så snabbt som möjligt för att kunna sätta motåtgärder.
25. **Sist men inte minst, utbilda dig.** Se till att du har åtminstone en god grundläggande kunskap i ämnet IT-säkerhet. Du hittar några bra länkar att börja med längre ner. Att du har läst ända hit är en riktigt bra början!

Ver. 2021 1.0

Tips på läsvärda och pålitliga länkar

Tjänster och verktyg

- **Kontrollera om din e-postadress eller ditt mobilnummer har funnits med i en dataläcka på Internet:** Have I Been Pwned: Check if your email has been compromised in a data breach
- **Kontrollera om en fil eller webbadress är skadlig:** VirusTotal - Home
- **Få hjälp och inspiration med att skapa en lösenordsfras:** Svenskt XKCD-lösenord (nyh.name)
- **Har du råkat ut för ett ransomware? Här kan du få hjälp:** Hem | The No More Ransom Project
- **DNS-filter (webbfilter)** Cisco har en tjänst som heter OpenDNS och fungerar som ett extra skydd mot skadliga och oönskade webbplatser. Ger även ett visst skydd mot phishing. En tjänst för ditt privata nätverk. Du hittar tjänsten här: Home Free by OpenDNS

Information och utbildning

- **Information om grundläggande IT-säkerhet:** Säker på internet – enkla tips för att öka it-säkerheten - Internetstiftelsen
- **Lösenord - Statistik, råd och rekommendationer för bättre säkerhet:** Rapport-Lösenord för alla (internetstiftelsen.se)
- **Hur kan jag undvika att bli lurad av nätfiske?** Så undviker du att bli lurad av nätfiske - Internetkunskap
- **Lär dig känna igen ett nätfiskemeddelande:** Skydda dig mot nätfiske (microsoft.com)
- **SSF: Sveriges nya samlingsplats för säkerhet online.** | Säkerhetskollen (sakerhetskollen.se)
- **MSB – Tänk säkert:** Tänk säkert (msb.se)
- **Skydda dig mot bedragare:** Skydda dig mot bedragare - Internetstiftelsen Ransom Project

Vill du veta mer om hur ni kan säkra er IT-miljö?

Vänligen kontakta: hej@primeq.se

Ver. 2021 1.0