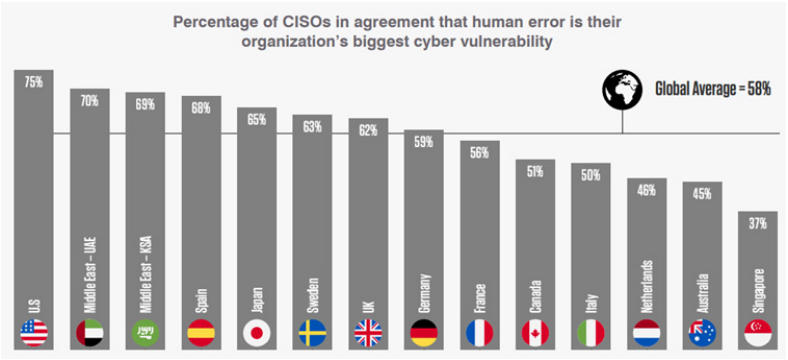
IT-säkerhet

Grundläggande IT-säkerhet för användare

63 procent av de svenska IT-säkerhetscheferna ser den mänskliga faktorn som deras största cybersårbarhet, något som kan kopplas till den utmaning som distansarbete inneburit för IT-säkerhetschefer.*

Användaren – den svagaste länken

I dagens moderna samhälle klarar vi oss inte längre utan en grundläggande kunskap i IT-säkerhet. Riskerna är helt enkelt för stora och hoten blir fler och fler. Ett framgångsrikt arbetssätt för att skydda oss och våra system kräver en kombination av tekniska systemskydd, rutiner men kanske framför allt kunskap. Den gamla klyschan "en kedja är aldrig starkare än sin svagaste länk" har sällan varit mer träffande än i fallet med IT-säkerhet. Tyvärr så är i många fall användaren den svagaste länken, och dessutom en förbisedd länk.



*Källa: Proofpoint, 2021 Voice of the CISO Report

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

Ver. 2021 1.0

PrimeQ

En partner. Många specialister.

Höj IT-säkerheten på ett enkelt sätt

I stället för att lösa katastrofen – förebygg den!
Den tekniska utmaningen att säkra system och plattformar blir mer utmanande i och med att komplexiteten ökar med fler system och användares krav på valmöjligheter gällande hårdvara och moderna molntjänster. Under corona-perioden har utmaningen blivit än större med snabba beslut på att ställa om till distansarbete. Lägg till en ökande tendens till ”shadow it” hos användare och problemet växer exponentiellt. Ett säkerhetssystem som kringgås, är farligare än att inte ha det alls, för man blir invaggad i falsk trygghet. Idag finns inte en säkerhetslösning som hanterar alla aspekter av de utmaningar vi står inför gällande malware, phishing, spam, ransomware, intrång, industrispionage, GDPR-krav, fysisk säkerhet, Schrems II, DDoS-attacker osv. Det finns dock en gemensam nämnare i ovan hot och det är användarna med deras kunskap och säkerhetsmedvetenhet (eller i många fall – bristen på kunskap). Ta vara på möjligheten att göra den största risken, till det starkaste skyddet och främsta tillgången i er IT-säkerhet. allvar. I stället för att lösa katastrofen – förebygg den!

Se dina användare som den viktigaste delen i ert IT-skydd
De flesta företag har redan idag ett grundläggande tekniskt skydd på plats. Det har investerats i smarta brandväggar, antivirus, spamfilter, DNS-skydd, kryptering, VPN osv. Så långt allt väl, men ofta missar man den lågt hängande frukten, nämligen utbildning av användarna. Genom att höja kunskapsnivån och säkerhetsmedvetandet hos användarna höjer du ert företags IT-säkerhet ordentligt. Vi vågar påstå att det är den mest kostnadseffektiva investeringen du kan göra gällande företagets IT-säkerhet. Se dina användare som den viktigaste delen i ert IT-skydd. Vi har tagit fram en generell lista med enkla tips för hur man som användare, både på kontoret och hemma, på ett enkelt sätt kan höja sin riskmedvetenhet och kunskap inom IT-relaterade frågor. Dessa åtgärder ersätter dock inte ett systematiskt säkerhetsarbete, men hjälper till att skapa en bra grund.

Ver. 2021 1.0

PrimeQ Torkel Knutssonsgatan 24, 6 tr, 118 49 Stockholm | Växel: 077-551 01 00 | E-post: hej@primeq.se | **primeq.se**

36 tips för bättre IT-säkerhet för användare

1. **Phishing.** Fall inte för nätfiske-fällan. Får du ett meddelande som du anser vara misstänkt, använd ditt sunda förnuft och kritiska tänkande. Verkar det hela logiskt, vem är avsändaren? Är det för bra för att vara sant? När du ser ett meddelande som manar till snabba åtgärder, se till att granska meddelandet noga. Är du säker på att det är äkta? Ta tid på dig och var försiktig. Klicka inte på länkar i misstänkta meddelanden, undersök i stället vart länken går genom att hovra (håll muspekaren över länken) och läs vart länken går. Läs även vår guide Phishing – 25 tips på hur du kan skydda dig

2. **Malware.** Öppna inte bifogade filer från okända avsändare eller om du meddelandet verkar misstänkt. Se till att du håller ditt operativsystem, applikationer och antivirusprogram uppdaterat. Läs även vår artikel Så skyddar du ditt företag mot utpressningsattacker - PrimeQ

3. **Dataläckage.** Undvik att mata in några uppgifter via formulär som länkats via e-post eller SMS.

4. **Nätverk.** Glöm inte IT-säkerheten hemma. Använd minst WPA2 som kryptering på ditt WiFi-nätverkt och välj en stark nätverksnyckel. Glöm inte att ändra standardlösenordet på din router och/eller trådlösa accesspunkter. Uppdatera till senaste firmware på samtliga enheter inklusive ev. IoT-enheter.

5. **Nätverk.** Använd inte öppna WiFi-nät eftersom den informationen skickas okrypterad och kan fångas av någon annan i nätverket. Det finns flera exempel på att öppna nätverk som erbjuds gratis sätts upp av bedragare. En fara är bl.a. att du i ett sådant nätverk inte kan lita på att du verkligen hamnar på den sida som du tror att du hamnar på. En inloggningssida för Facebook kan vara en förfalskad version och fyller du i dina inloggningsuppgifter så hamnar de i bedragarnas händer.

6. **Fysisk säkerhet.** En ofta förbisedd men viktig faktor i IT-säkerheten. Lås på dörrar, skalskydd och larm är givet ur flera aspekter. Mindre uppenbara är kanske tillgång till nätverksuttag, kameraskydd på laptop och lås på postlåda. Släng inte papper med känsliga data i pappersåtervinningen utan att riva sönder dem eller köra dem genom dokumentförstöraren.

7. **Fysisk säkerhet.** Vem tittar över din axel? Var försiktig när du till exempel sitter på tunnelbanan och skriver in ditt lösenord eller behandlar känsliga uppgifter. Arbetar du med känsliga uppgifter på offentliga platser kan det vara bra att investera i ett sekretessfilter till skärmen.

Ver. 2021 1.0

36 tips för bättre IT-säkerhet för användare

8. **Fysisk säkerhet.** Hämta dina utskrifter direkt och låt dem inte ligga kvar i skrivaren. Glöm inte heller dokumentet som du lagt i scannern för att scanna.

9. **Surfa säkert.** Använd en DNS-tjänst med inbyggt webbfilter. Detta fungerar som ett extra skydd mot skadliga och oönskade webbplatser. Ger även ett visst skydd mot phishing. En tjänst för ditt privata nätverk. Läs mer under Tjänster & verktyg längre ner.

10. **Backup.** En viktig detalj om olyckan är framme och du drabbas av kryptovirus eller annan skadlig kod som innebär att du behöver installera om hela datorn. Se till att du sparar filerna på ett helt separerat system.

11. **Källkritik.** Var kritisk till information på Internet och förstå när du ska ha källtillit. Deepfake är ett exempel hur svårt det kan vara att lite på vad du ser och hör. Deepfake är förfalskningar som är grundligt gjorda och väldigt genomarbetade. Här är ett exempel på konsekvenser av detta: A Voice Deepfake Was Used To Scam A CEO Out Of $243,000 (forbes.com)

12. **Behörigheter.** Var restriktiv med att ge behörighet till tjänster som använder andra tjänsters autentisering. T.ex. Facebook, Google, Apple eller Microsoft 365.

Andel företag i Sverige som saknar kompetens och resurser för att klara cybersäkerhetshot: 50 procent Källa: Teknikföretagen, Skydda din IT-miljö - En guide till medvetet säkerhetsarbete i mindre teknikföretag

13. **Generellt.** Ladda inte ner okända program eller appar. Avinstallera program du inte använder.

14. **Generellt.** Fundera över vad du delar på sociala medier och vad du skriver. Skilj på din roll som anställd och din privatperson. Var medveten om att allt du gör kan spåras.

15. **Generellt.** Lås alltid skärmen när du lämnar din dator (tips för Windows-användare är kortkommandot ”Win+L”)

16. **Generellt.** Behandla även kasserad IT-utrustning som bärare av känslig information. En trasig dators hårddisk kan enkelt kopplas in i annan utrustning och den sparade informationen kan enkelt läsas av obehöriga.

17. **Generellt.** Var försiktig med USB-produkter som kopplas in till datorn. Ett USB-minne kan innehålla skadlig kod.

PrimeQ **PrimeQ** Torkel Knutssonsgatan 24, 6 tr, 118 49 Stockholm | Växel: 077-551 01 00 | E-post: hej@primeq.se | primeq.se

36 tips för bättre IT-säkerhet för användare

18. **Generellt.** Betrakta din personliga information som känslig data. Dela inte med dig av uppgifter i onödan.

19. **Mobil.** Glöm inte att din mobil i princip är en bärbar dator. Skydda den därefter. Många av punkterna i denna lista gäller även din mobil eller padda. Läs även vår artikel Fem gånger vanligare med mobila hot i Sverige än resten av världen - PrimeQ

20. **ID-kapning.** Skydda dig mot ID-kapning. Skatteverket har en tjänst där du i förebyggande syfte kan spärra din adressändring så att den endast kan ändras om du identifierar dig med din e-legitimation. Här hittar du tjänsten. Svensk Adressändring har även tjänsten Adresslåset möjliggör en spärr på din postadressändring med hjälp av BankID. Spärren är kostnadsfri och gäller för beställningar av Svensk Adressändrings tjänster. Här hittar du tjänsten. Se även till att aktivera notiser på mobilt Bank-ID och i Kivra. Läs även vår artikel Skatteverket och polisen uppmanar till att aktivera spärrar som skydd mot ID-kapning - PrimeQ

21. **ID-kapning.** Logga aldrig in via ditt Bank-ID eller bankdosa på uppmaning av någon annan. Läs mer på Grovt oaktsamt eller särskilt klandervärt (konsumenternas.se)

    Om du har lämnat ut kortuppgifter via ett phishingmail har du enligt Allmänna reklamationsnämndens, ARN:s, praxis i vart fall agerat grovt oaktsamt och då har konsumenter själva fått stå för 12 000 kr. Om man lämnat ut flera inloggningskoder via sociala medier eller låtit någon okänd person fjärrstyra ens dator har ARN slagit fast att konsumenterna till och med har agerat särskilt klandervärt. De har då fått stå för hela beloppet. Läs mer på Grovt oaktsamt eller särskilt klandervärt (konsumenternas.se)

22. **Lösenord.** Använd MFA (multifaktorautentisering) eller passwordless på alla tjänster där det finns stöd för detta.

23. **Lösenord.** Använd inte samma lösenord till flera tjänster. Har tjänsten inte stöd för MFA (multifaktorautentisering) bör du använda olika lösenord (eller ännu hellre – lösenfraser, mer om det senare).

24. **Lösenord.** Använd en pålitlig lösenordshanterare så att du slipper skriva ner lösenord på en post-it-lapp under tangentbordet (jo det händer fortfarande...)

Ver. 2021 1.0

36 tips för bättre IT-säkerhet för användare

25. **Lösenord.** Svara inte på ”roliga” tester eller frågor av typen ”Vilken var din första bil?”, ”Vad hette ditt första husdjur?” eller ”Minns du ditt första telefonnummer?” på Sociala medier. Känner du igen frågorna? Precis – det är samma typ av frågor vissa molntjänster använder för återställning av lösenord. Ge inte bort personlig information till vem som helst på Internet.

26. **Lösenord.** Använd lösenordsfras i stället för ett lösenord. Det blir mycket svårare för en bedragare att knäcka ditt lösenord genom att låta automatiserade program prova möjliga kombinationer. Det är dessutom enklare att komma ihåg en ett krångligt påhittat lösenord.

27. **Spam.** Svara aldrig på ett spam. Då bekräftar du bara att din e-postadress fungerar och du riskerar att få ännu mer skräppost.

28. **Spam.** Ställ in ditt e-postprogram på att inte automatiskt ladda ner bilder, eftersom de också kan bekräfta att din adress fungerar.

29. **Spam.** Avregistrera dig inte från suspekta nyhetsbrev – spärra dem i stället i din e-postklient. Om du avregistrerar dig talar du om för avsändaren att e-postadressen eller mobilnumret används.

30. **Uppdatera.** Uppdatera ditt antivirusprogram. Även om antivirusprogram inte upptäcker all skadlig kod fyller de fortfarande en funktion. Se till att ditt program är uppdaterat med de senaste signaturerna för att öka möjligheten att stoppa skadlig kod.

31. **Uppdatera.** Håll operativsystem, webbläsare och insticksprogram uppdaterade. Bedragare utnyttjar gärna kända säkerhetsbrister i både operativsystem och webbläsare, men framför allt i insticksprogram som till exempel Java och Adobe Flash. Du bör uppdatera så fort du får en notifiering om att nyare versioner finns tillgängliga.

32. **Kunskap.** Ta hjälp av betrodda bra tjänster på Internet. Du hittar några exempellänkar i slutet av denna lista.

33. **Kunskap.** Läs och följ ditt företags IT-policy. Läs även vår artikel 10 konkreta tips vid digitalisering - PrimeQ

Svenska näringslivets kostnader för cyberattacker är cirka 16 miljarder per år. Källa Teknikföretagen, Cyberhoten - så ser hotbilden och attackerna ut mot svenska teknikforetag

Ver. 2021 1.0

36 tips för bättre IT-säkerhet för användare

34. **Kunskap.** Håll dig uppdaterad om aktuella säkerhetshot. Du hittar några bra pålitliga källor i slutet av denna lista.

35. **Kunskap.** Är du osäker? 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 in motåtgärder.

36. **Kunskap.** Sist men inte minst, utbilda dig. Se till att du har åtminstone en god grundläggande kunskap i ämnet IT-säkerhet. Kom ihåg att kunskap är en färskvara, håll dig informerad och fortsätt vara vaksam. Du hittar några bra länkar att börja med längre ner. Att du har läst ända hit en riktigt bra början!

Vill du som arbetsgivare utbilda dina användare och höja riskmedvetenheten för att höja IT-säkerheten i ditt företag? Läs mer om vår automatiserade tjänst PrimeQ Security Awareness Training.

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