Hackare bryter sig inte in – de loggar in

Secured By Telia Cygate

Sju steg som stänger cyberbrottslingen ute

Hela 98 procent av alla cyberattacker bygger på social manipulation. Hoten utgår sällan från avancerad kod eller teknik, utan från hur vi människor fungerar. Medarbetaren som vill hjälpa en kollega, chefen som har bråttom, eller föräldern som lånar ut datorn till sitt barn. Det är dörren in för cyberbrottslingen. För att inte låta oss luras behöver vi förstå våra mänskliga egenskaper, träna oss på att stå emot och skapa förutsättningar för teknik och människa att gå hand i hand.

> ***"Det är lättare att hacka en människa än en dator"***
>
> Anne-Marie Eklund Löwinder (Amel), CEO and Cyber Security Expert.

I den här guiden får du koll på människan som attackyta, och hur du kan skydda dig och din organisation.

Känslor öppnar dörrar

1. **Vanlig fälla:** Människor har en stark drivkraft att vara en del av gruppen och att få veta vad som händer. Du har säkert hört talas om fenomenet *"Fear of Missing Out (FOMO)"*, och det är precis den typen av beteende som bedragare älskar att utnyttja. Det är FOMO som gör att vi får puls av mejl med rubriken "Så påverkas du av omorganisationen" eller av ett sms om en obetald faktura på väg till inkasso.

Så skyddar du dig: De flesta av oss är inte medvetna om hur mycket känslor som oro, rädsla och nyfikenhet påverkar våra beslut. Reflektion och eftertanke kring hur känslorna påverkar oss är minst lika viktiga komponenter av en stark säkerhetsstrategi som brandvägg och uppdaterat virusskydd.

Stress gör dig korkad

2.

Vanlig fälla: Vem vill inte vara effektiv och leverera snabbt? Men ett högt tempo och stress kan leda till farliga genvägar. Vi återanvänder lösenord och hoppar över säkerhetsrutiner. Och när det är bråttom, riskerar vi att skanna falska QR-koder och ladda ner osäkra appar. Det här vet cyberbrottslingarna, och skapar upplevelsen av brådska för att lura dig.

Så skyddar du dig: För att inte riskera att brådskan öppnar dörren på vid gavel behöver vi prata om vikten av att stanna upp. Och vara tydliga med att det är bättre att missa en deadline eller logga in senare, för att säkerställa att det sker säkert. Multifaktorautentisering är ett bra exempel på när vi tvingas tänka till, ta ett extra steg och agera med eftertanke.

Hjälp inte hackaren

3.

Vanlig fälla: Hjälpsamhet är en styrka i arbetslivet, men också en svaghet som angripare utnyttjar. Vi vill gärna vara till lags. Därför klickar vi, delar och öppnar – både digitala och fysiska dörrar. Ett mejl från ”chefen” som snabbt behöver hjälp med att betala en faktura eller en ”kollega” som ber oss om en tjänst för att ”hinna leverera” kan få oss att agera utan eftertanke.

Så skyddar du dig: Lösningen är inte att sluta vara hjälpsam, utan att träna på att vara det på ett säkert sätt. Skapa en kultur på arbetsplatsen där vi uppmuntrar till sunt ifrågasättande, och där vi regelbundet simulerar attacker för att öva på hur man ska agera när det verkligen gäller.

91 %

av alla organisationer rapporterade minst en cyberincident eller ett dataintrång under 2022.

52 %

Mer än hälften av alla ledare, anser att deras medarbetare saknar tillräcklig cybersäkerhetskunskap.

Vanskliga vanor i en digital vardag

4.

Vanlig fälla: Distansarbete, öppna wifi-nätverk och sjuka barn som kan spela på jobbdatorn är bekvämt för vardagspusslet. Tyvärr tycker hackaren också att det är toppen. Ju mer vi blandar arbetsliv med privatliv, och tar smidiga genvägar med ny teknik, desto fler öppningar skapas för angripare.

Så skyddar du dig: Säkerhet måste fungera i vardagen – inte bara i teorin. Medarbetare behöver förstå riskerna i sina beteenden och få tillgång till säkra och användarvänliga alternativ. När vi gör säkerhet till en naturlig del av vardagen, som till exempel med enkla rutiner för rapportering av angrepp och lättförståeliga policyer för hur jobbdatorn får användas, blir hackarens jobb betydligt svårare.

AI grumlar gränsen mellan sant och falskt

5.

Vanlig fälla: Vi litar på det vi ser och hör. Just därför är deepfakes och röstkloning så farliga. Videomeddelandet från chefen kan se trovärdigt ut, och rösten i telefon kan låta precis som en kollegas – men båda kan vara AI-genererade.

Så skyddar du dig: För att stå emot tekniskt avancerad manipulation måste det bli en vana att verifiera och dubbelkolla. Ingenting ska slinka igenom bara för att det verkar trovärdigt. Vi behöver påminna varandra att ta den extra kontrollen, och acceptera att det ibland får ta lite längre tid. Det är även viktigt att vi kontinuerligt utbildar oss och håller oss uppdaterade, särskilt när ny teknik ständigt förändrar hotbilden.

Alla gör som chefen

6.

Vanlig fälla: Regler som inte tillämpas i vardagen gör liten nytta, även om de i grunden är vettiga och godkända av ledningen. Och om ledare öppet bryter mot reglerna, som att lämna datorn olåst i konferensrummet eller dela lösenord i ett mejl, får policyerna aldrig någon kraft.

Så skyddar du dig: När chefer visar vägen, förankrar tydliga säkerhetspolicyer och själva följer dem blir det enklare för alla att agera rätt. Det handlar inte om pekpinnar, utan om att skapa regler som känns meningsfulla och efterlevs i vardagen. När ledningen följer regler på ett självklart sätt blir hela organisationen den starkaste länken.

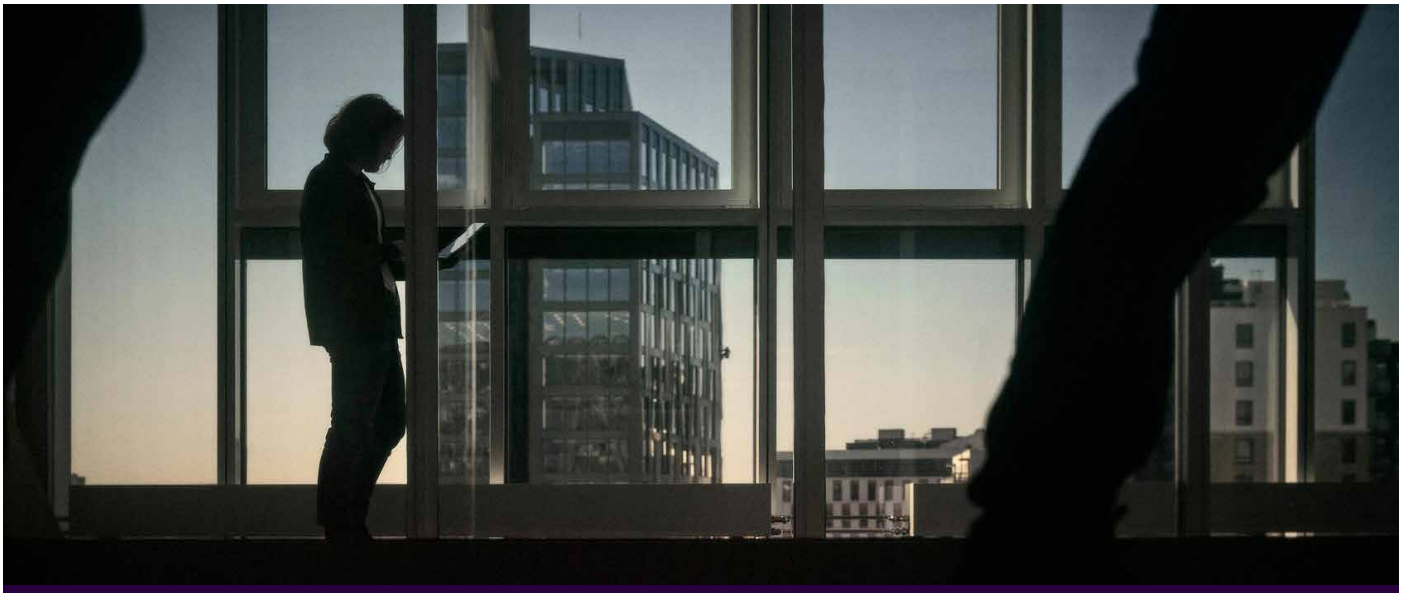
Organisationer som bygger en stark säkerhetskultur ökar sin resiliens med 46 %

Skammen är hackarens bästa vän

7.

Vanlig fälla: Det är pinsamt att ertappas med att ha gjort fel. Oavsett om vi tog en genväg runt en säkerhetsrutin eller blev lurade. Många som trillat dit skäms i det tysta. Men tystnaden är farlig och ger angripare ett försprång.

Så skyddar ni er: Skapa en kultur där det är tryggt att göra misstag och okej att prata om dem. Träna på att bryta impulsen att dölja fel och gör det enkelt att rapportera misstänkta händelser. Då kan organisationen stoppa angrepp i tid, lära av det som hänt och bygga starkare rutiner för framtiden.



Bygg en säkerhetsmedveten organisation

- ✓ Utbilda kontinuerligt och öva på verkliga hot
- ✓ Gör det enkelt att rapportera misstänkta händelser
- ✓ Ha en tydlig och pedagogisk säkerhetspolicy
- ✓ Låt säkerheten styra tempot
- ✓ Skapa en kultur där misstag är okej

Telia och Telia Cygate – Unik kombination av erfarenhet och expertis

Vi kombinerar säkra nät med djup teknisk kompetens inom cybersäkerhet. Som en del av totalförsvaret har vi en unik position där vi både skyddar samhällskritisk infrastruktur och stärker företags digitala motståndskraft i vardagen. Genom att förena förståelse för teknik, människor och organisationer bidrar vi till ett säkrare och mer robust digitalt Sverige. Läs mer på: telia.se/foretag/erbjudanden/sakerhet

Informationen i den här guiden är hämtad från Buckle up! Telia Trend Report 2024

Secured By Telia Cygate