Guide för träning inom säkerhets-medvetenhet

Innehåll

Hur attacker med människor som måltavla utvecklas 02

Varför mänskliga misstag är den största säkerhetsrisken 03

Hur sker mänskliga misstag? 04

Hur kan anställda göra säkrare beslut i vardagen? 05

Hur man håller personalen säkerhetsmedveten vid distansarbete 06

Hur säkerheten fungerar vid arbete hemifrån 07

Det bästa formatet för träning inom säkerhetsmedvetenhet 08

Old-school träning vs. modern träning 08

Hur man gör modern träning effektiv 09

Hur man bäddar in säkerhetsmedvetenhet i personalens vardag 10

Hur man bygger en kultur kring säkerhetsmedvetenhet 11

Nödvändiga ämnen inom säkerhetsmedvetenhet 12-15

Att komma igång 16

Inledning

Hur attacker med människor som måltavla utvecklas

Coronapandemin har skapat många nya utmaningar när det kommer till säkerhetsmedvetenhet. Företag i världen har anpassat sig genom att arbeta hemifrån och distansera sig, medan de har behövt hantera nya hot från cyberkriminella som utnyttjat rädsla och nyfikenhet. Samtidigt som företag har hanterat dessa nya utmaningar, så har klassiska cyberhot varit mer förekommande än någonsin.

Bland de största cyberhoten är skadlig kod fortfarande en fara. Utbrottet av WannaCry 2017 som kostade företag i världen över 4 miljarder dollar är fortfarande i färskt minne, och andra nya stammar av skadlig kod upptäcks dagligen.

Phishing har också fått ett uppsving under de senaste åren, och många nya bedrägerier har uppfunnits för att dra nytta av intet ont anande företag. Varianten CEO Fraud-bedrägeriet som skedde via e-post, kostade enbart brittiska företag 14,8 miljoner pund under 2018.

Personal som arbetar hemifrån står utanför IT-supportteamens direkta tillsyn och har ofta svårt att hantera cyberhot och skydda företagsinformation på lämpligt sätt.

Att inte uppdatera programvara och operativsystem, att skicka data via osäkra nätverk och att i allt större utsträckning använda e-post och online-meddelanden har gjort de anställda mycket mer mottagliga för hot som skadlig kod och phishing.

Tekniska lösningar som skräppostfilter och system för hantering av mobila enheter är viktiga för att skydda slutanvändarna. Med tanke på antalet hot och den mängd system och kommunikation som personalen arbetar med, är dock den största riskfaktorn den mänskliga faktorn.

Varför mänskliga fel är den största säkerhetsrisken för ditt företag

Nästan alla cyberintrång har en variabel gemensamt: mänskligt fel. Mänskliga fel kan yttra sig på många olika sätt: allt från att inte installera säkerhetsuppdateringar i tid till att ha svaga lösenord och lämna ut känslig information i phishingmejl.

Även om modern programvara för att motverka skadlig kod och upptäcka hot har blivit mer sofistikerad, vet cyberbrottslingar att tekniska säkerhetsåtgärder bara är effektiva om de används på rätt sätt av människor.

Om en cyberbrottsling lyckas gissa lösenordet till en företagsportal på nätet, eller använder social engineering för att få en anställd att göra en betalning till ett bankkonto, finns det inget som tekniska lösningar kan göra för att stoppa intrånget.

År 2014 genomförde IBM en undersökning av de cyberintrång som inträffade bland tusentals av deras kunder i över 130 länder. Denna studie var den mest omfattande granskning av orsakerna till cyberintrång som hade gjorts vid den tidpunkten, men dess resultat har sedan dess bekräftats av liknande studier.

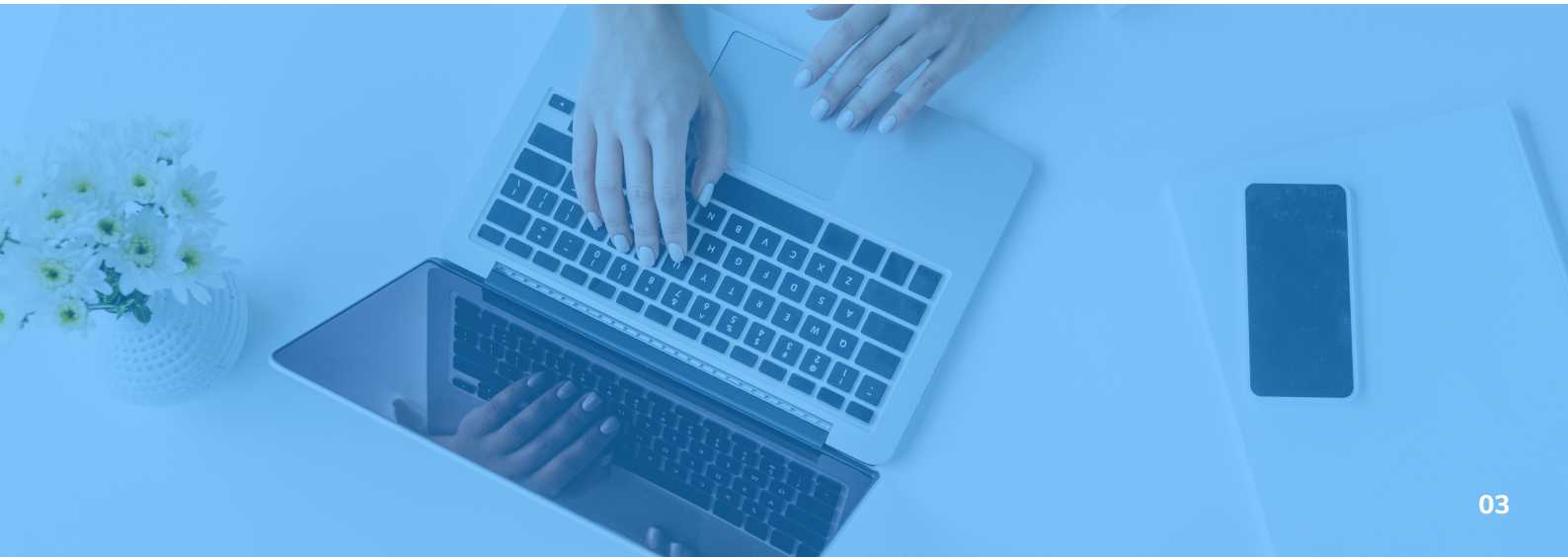
En av de viktigaste slutsatserna i IBM:s studie var att mänskliga fel var en viktig bidragande orsak vid 95 procent av alla intrång.

Med andra ord, om mänskliga fel inte hade varit en faktor är det troligt att 19 av de 20 överträdelser som analyserades i studien inte skulle ha inträffat överhuvudtaget.

"Mänskliga fel var en bidragande faktor till 95 % av alla överträdelser"

Eftersom mänskliga fel spelar en så stor roll i cyberbrott är det viktigt att ta itu med dem för att minska risken för att ditt företag ska bli måltavla. Det ger dig också möjlighet att skydda ditt företag från ett mycket bredare spektrum av hot än vad en enskild teknisk lösning skulle kunna göra - och kan potentiellt ge din personal möjlighet att aktivt hålla utkik efter och rapportera nya hot som de kan stöta på.

Att minska mänskliga fel bör vara centralt för moderna företag - och i nästa avsnitt ska vi titta på de bästa sätten att göra det på.



När sker mänskliga fel?

Det måste finnas två faktorer för att ett mänskligt fel ska kunna uppstå: möjlighet och beslut. Möjlighet innebär att det finns en situation där en människa tillåts göra ett misstag: till exempel att låta slutanvändarna hantera programuppdateringar i stället för att automatiskt installera nya säkerhetsuppdateringar. Beslut är individens handling: i situationen ovan tillåter bristen på handling det mänskliga felet - att inte installera säkerhetsuppdateringar när de finns tillgängliga.

Begränsningsåtgärder minskar möjlighet till fel, samt förbättrar slutanvändarnas beslut. Det är viktigt att vidta åtgärder inom båda områden för att se till att mänskliga fel åtgärdas på ett grundligt sätt.

När det gäller patchning kan en teknisk åtgärd som att införa patchhantering minska möjligheten till mänskliga fel. Det är dock fortfarande viktigt att ta hänsyn till situationer där tekniska lösningar tillfälligt upphör, eller om en ny policy införs (t.ex en BYOD-policy där användarna tillåts använda sina egna enheter utan patchhantering).

I andra fall, t.ex. vid phishing, har tekniska åtgärder som skräppostfilter en mycket begränsad effekt när det gäller att minska möjligheten till fel. Vid målinriktade phishing-attacker är det enda effektiva sättet att minska mänskliga fel att lära slutanvändarna att göra bättre bedömningar.

"Det måste finnas två faktorer för att ett mänskligt fel ska kunna uppstå: möjlighet och beslut."

Hur kan anställda fatta bättre säkerhetsbeslut i vardagen?

1 Förståelse

Användaren måste inse att han eller hon befinner sig i en situation där säkerheten potentiellt står på spel. Om användaren inte inser detta kanske personen inte ens inser att han/hon fattar ett beslut genom sin passivitet.

2 Empowerment

Användaren måste veta vad som är rätt tillvägagångssätt. Detta kräver inte nödvändigtvis att användaren förstår hotet fullständigt, utan är ofta är det så enkelt som att rapportera situationen till en person på IT- eller säkerhetsavdelningen som kan undersöka den.

3 Utbildning

Användaren måste veta varför säkerheten är viktig, så att de förstår vikten av att inte ignorera säkerhetsrutinerna och är medvetna om de potentiella konsekvenserna av en överträdelse.

4 Eliminera "pain avoidance"

Problem som bristande lösenordssäkerhet och bristande patching av programvara förekommer fortfarande i organisationer över hela världen, trots att många datoranvändare förstår varför dessa frågor är kritiska för säkerheten. Anledningen till att man inte vidtar åtgärder trots att man känner till dem är att man undviker den energi det tar, vilket kallas för "pain avoidance". Att ha ett unikt och starkt lösenord kräver mer tid att skapa och mer ansträngning att komma ihåg än ett kort, svagt eller återanvänt lösenord.

Trots att användaren vet bättre är den "smärta" som orsakas av att skapa ett starkt lösenord ofta tillräckligt stark för att få användaren att gå emot sitt bästa omdöme. Detta förvärras av det faktum att även om många användare vid optimala förhållanden vidtar rätt åtgärder, kan upptagna och brådskande arbetssituationer samt stress göra att säkerhetsåtgärderna känns ännu mer "smärtsamma" för användarna.

Slutanvändarna måste känna att den smärta som orsakas av att följa bästa säkerhetsrutiner är mindre än den tillfredsställelse man får om man inte gör det. Tekniska åtgärder som lösenordshanterare är viktiga i detta sammanhang, eftersom de gör det mycket lättare att agera på ett säkert sätt: om de anställda inte behöver skapa eller komma ihåg sina egna lösenord har de ingen anledning att inte använda säkra lösenord.

Samtidigt måste tröskeln för att utföra rätt handling genom kulturell förändring bli mindre. Detta innebär att säkerheten måste sättas i förgrunden vid beslutsfattandet och att man måste se till att användarna aldrig känner att de "slösar tid" genom att vidta lämpliga säkerhetsåtgärder.

En effektiv utbildning i säkerhetsmedvetenhet tar upp inte bara en, utan alla fyra faktorerna. Det innebär att man identifierar situationer där uppgifter eller system kan äventyras, förstår bästa praxis, vet vilka de potentiella konsekvenserna av överträdelser är och slutligen hjälper till att driva igenom en kulturell förändring för att skapa en miljö där säkerhetsöverväganden alltid tas med i beslutsfattandet.

Säkerhetsmedvetenhet i hemmet

Håll personalen säkerhetsmedveten vid arbete hemifrån

Den globala reaktionen på Covid-19 har orsakat många förändringar på arbetsplatserna. Den förändring som har haft störst inverkan på säkerheten har varit att många företag på kort tid har övergått till att låta de flesta eller alla anställda arbeta hemifrån. Detta har i sin tur lett till att många slutanvändare löper större risk att utsättas för hot på nätet.

Anställda som inte var vana vid att arbeta hemifrån före pandemin upptäckte snabbt några av de problem som det skulle medföra: att ta hand om barn och husdjur, hantera dålig internetuppkoppling och stå ut med alla andra störningar som kan uppstå i hemmet. Mitt i alla dessa nya förändringar av arbetsmiljön hamnade säkerheten ofta långt ner på användarnas prioriteringslista.

Slutanvändare som arbetar hemifrån har inte tillgång till IT-support och kan ha svårt att lösa enkla tekniska problem. Dessutom har viktiga säkerhetsuppgifter tilldelats slutanvändarna - exempelvis uppdatering av programvara och operativsystem, uppdatering av fast programvara för routrar och säkring av nätverket.

Det är inte konstigt att cyberbrottslingar inte har slösat en sekund på att utnyttja pandemins omständigheter för att hitta på nya former av bedrägerier och cyberbrottslighet.

Mitt i alla dessa nya förändringar i arbetsmiljön hamnade säkerheten alltför ofta längst ner på användarnas prioriteringslista.

Hur man hanterar säkerheten vid arbete hemifrån

IT-supportteamet kan inte vara hemma hos alla slutanvändare, och därför är det viktigt att se till att slutanvändarna är medvetna om sitt eget ansvar för att upprätthålla säkerheten. Slutanvändarna måste veta att de är ansvariga för att se till att de endast får tillgång till företagets information och nätverk via enheter och nätverk som är uppdaterade och säkra.

Utbildning i säkerhetsmedvetenhet är nyckeln till att se till att slutanvändarna vet hur de ska upprätthålla säkerheten. Det är bäst att dela upp utbildningen i små, lättsmälta delar, eftersom detta säkerställer att användarna inte blir överväldigade. Utbildningen bör också äga rum regelbundet - minst en gång i månaden - för att säkerställa att de viktigaste kunskaperna behålls och att användarna inte glömmer bort säkerheten så fort nästa arbetsprojekt kommer som skakar om prioriteringslistan. Slutligen är det viktigt att testa slutanvändarna.

Det bör klargöras att detta inte är ett sätt att döma eller bestraffa användare som har problem att klara träningen. Detta är snarare ett sätt att identifiera viktiga säkerhetsluckor i arbetsstyrkan och åtgärda dem innan de kan utnyttjas av cyberbrottslingar.

"Utbildning inom säkerhetsmedveten het är nyckeln till att slutanvändarna vet hur man upprätthåller säkerheten."

Old school VS modern träning

Hur man väljer det bästa formatet för utbildning inom säkerhetsmedvetenhet

All utbildning i säkerhetsmedvetenhet har inte samma format. Det sätt på vilket utbildningen genomförs, struktureras och presenteras har stor betydelse för hur effektiv den är när det gäller att förbättra säkerhetsresultaten i din organisation. I det här avsnittet tar vi en titt på exakt vad som är det bästa sättet att utföra utbildning i säkerhetsmedvetenhet för dina slutanvändare.

Utbildning i säkerhetsmedvetenhet har tidigare inneburit att slutanvändare fick sitta på en årlig session med timmar av föreläsningar och bildspel. Tanken var att användarna skulle komma ihåg det de såg och hörde - och i värsta fall kunde åtminstone "utbildning av användare" checkas av på listan. Men hur förbättrades säkerhetsresultaten? Det fungerade inte, och alla hatade formatet.

Varför utbildning som hålls årligen misslyckas

Det finns ett antal skäl till varför denna typ av årlig föreläsningsbaserad utbildning inte är effektiv.

Det första skälet är att en årlig utbildningssession helt enkelt innehåller för mycket information på en gång för att en anställd ska kunna smälta och komma ihåg den.

Även om användarna får läromedel att ta med sig eller om de får påminnelser vid enstaka tillfällen, är det troligt att det mesta av materialet under utbildningstillfället kommer att gå in genom ena örat och ut genom det andra - det kommer att glömmas bort på bara några ögonblick.

Föreläsningar och presentationer är helt enkelt inte engagerande format för slutanvändare. De lyckas inte väcka de anställdas intresse på samma sätt som video och interaktivt innehåll gör, och alltför ofta är de fyllda med onödig information som inte är relevant för alla slutanvändare.

Slides som är fyllda till bredden med liten text kommer garanterat att få vilken anställd som helst att somna halvvägs genom sessionen.

Det sista viktiga skälet till att traditionell träning inte är effektiv är att den inte använder sig av inlärning genom upprepning. Om det går ett år mellan utbildningstillfällena kommer användarna helt enkelt inte ihåg vad de har lärt sig. Säkerheten kan inte vara en engångsföreteelse, utan måste vara något som tränas under hela året.

Utbildning i säkerhetsmedvetenhet har i allt högre grad övergått till lösningar med mjukvara som en tjänst på nätet. Molnbaserad utbildning ger vissa omedelbara fördelar jämfört med traditionella metoder, men är inte nödvändigtvis den ultimata lösningen på säkerhetsmedvetenhet om den inte levererar på vissa områden som är viktiga för att verkligen förbättra säkerhetsresultaten.

Hur man kan göra modern träning effektiv

Dela upp materialet

Det finns en begränsad mängd information som en person kan ta till sig åt gången. För att inte överväldiga slutanvändarna bör utbildningen delas upp i segment, vart och ett med ett eget tydligt och enkelt budskap som presenteras på ett lättsmält sätt.

Fortgående utbildning

Genom att dela upp materialet kan man också enkelt göra inlärningen kontinuerlig, snarare än en engångsföreteelse, och kurser kan skickas ut regelbundet under året, vilket hjälper till att hålla säkerhetsmedvetenheten ständigt närvarande hos slutanvändarna.

Relevant material

När en slutanvändare får information som han eller hon inte tycker är relevant kommer personen snabbt att förlora intresset och bli mindre uppmärksam. Läromaterialet bör inte bara undvika jargong och tekniska termer, utan också vara utformat med tanke på verkliga situationer som slutanvändaren kan råka ut för.

Gör säkerhet en del av företagets kultur

Träning måste bli en del av företagets kultiur, där säkerhetsmedvetenhet alltid tas i beaktande och där användarna uppmuntras att ställa frågor och ta upp problem.

Ge praktiska råd

Det är viktigt att medarbetarna går från utbildningen med konkreta åtgärder i åtanke som de kan använda direkt i sitt dagliga arbete. Att ge medarbetarna chansen att testa utbildningen direkt hjälper också till att bygga upp minnet, och det kan göras med hjälp av verktyg som phishing-simulering.

Video och interaktivt innehåll

Video och interaktivt innehåll är bra för att engagera användare som kanske föredrar en annan typ av inlärningsupplevelse. Många människor lär sig genom att göra, svara på frågor eller på annat sätt delta.

Mäta påverkan av träning

Det är viktigt att användarna testas på vad de har lärt sig efter utbildningstillfällena. Detta hjälper dig att veta att användarna går därifrån och har lärt sig något - men det underlättar också användarnas inlärningsprocess.

Att bygga en säkerhetsmedveten kultur

Hur man bäddar in säkerhet i personalens vardag

Utbildning i säkerhetsmedvetenhet är inte effektiv när det gäller att förbättra säkerhetsresultaten om den inte åtföljs av en kulturell förändring. Omfattande utbildning lär slutanvändarna hur de ska känna igen situationer där säkerheten är hotad och hur de ska hantera dem på lämpligt sätt - men denna kunskap kommer inte att omsättas i praktiken om inte användaren känner att säkerheten värderas i deras kultur.

Med tanke på det ökande antalet hot, den ökande komplexiteten hos företagstjänster och tillgång till data och system från mobila enheter så är det omöjligt att veta var nästa hot eller oavsiktliga läcka kan dyka upp.

Därför bör säkerheten inte handla om att se till att slutanvändarna väljer starka lösenord eller följer andra specifika steg - utan snarare om att ge dem möjlighet att vara aktiva väktare av ditt företag, dess system, enheter och data.

"Omfattande utbildning lär slutanvändarna hur de ska känna igen situationer där säkerheten är i fara och hur de ska hantera dem på lämpligt sätt - men denna kunskap kommer inte att omsättas i praktiken om inte användaren känner att säkerheten värderas i företagets kultur."

Att bygga en säkerhetsmedveten företagskultur

Få stöd från högsta ledningen

Kulturförändringar och företagets värderingar måste komma uppifrån. Den högsta ledningen är viktig när det gäller att betona säkerhetens roll i verksamheten - men det är viktigt att den nya kulturen växer fram, snarare än att den dikteras.

Detta innebär att man måste uppmuntra de anställda att ta en aktiv roll genom att be dem ta upp frågor som rör deras egna roller och uppmana dem att ställa frågor och engagera sig i säkerhetsfrågor. På så sätt känner användarna att de är delaktiga i säkerhetsprocessen och börjar aktivt tänka på säkerhetsaspekterna i sina egna roller.

Tillträde med minsta möjliga privilegier

Principen om minsta möjliga privilegier ses ofta som en teknisk åtgärd - att begränsa varje användare till endast de privilegier som de behöver för sina specifika arbetsuppgifter - men den bör också förankras direkt i företagskulturen.

Detta innebär att man uppmuntrar användarna att aktivt rapportera när de har tillgång till fler uppgifter eller system än vad de behöver, vilket bidrar till att begränsa möjligheterna till överträdelser.

Fysisk säkerhet

När det gäller fysiska åtgärder kan affischer vara till hjälp för att skapa en säkerhetskultur, och de kan också innehålla användbara påminnelser om t.ex. lösenordsstyrka.

Det är dock viktigt att komma ihåg att det inte räcker att bara sätta upp en affisch på väggen för att åstadkomma något i sig. Affischerna bör användas som diskussionsunderlag eller som ett komplement till utbildningsmaterial som användarna redan är engagerade i.

Viktiga diskussionsämnen

Vilka ämnen är viktigast att ta upp inom säkerhetsträning?

Även om varje organisation och varje arbetsroll har olika krav finns det några viktiga områden som alla slutanvändare bör känna till.

Topp-12 ämnen för träning:

1. Phishing-tekniker
2. Social Engineering
3. Säkerhet hemma
4. Säkerhet på e-mail & internet
5. Arbeta på distans
6. Säkerhet på mobila enheter
7. Lösenord och autentisering
8. Säkerhet i molnet
9. Allmänt Wi-Fi
10. Fysisk säkerhet
11. Flyttbar media
12. Användning av sociala medier

#1. Tekniker för phishing

Phishing är fortfarande ett stort hot. En av anledningarna till att nätfiske är så populärt bland cyberbrottslingar är att det lätt kan anpassas för att utnyttja en händelse eller omständighet - som Covid-19-pandemin - för att rikta in sig på användare med nya bedrägerier. Mallbaserade bedrägerier som erbjuder information till offren har blivit populärare än någonsin - medan spear-phishing-attacker som riktar sig till enskilda användare och företag fortfarande är den farligaste sorten.

Slutanvändare är mest mottagliga för phishingmejl som skapar en känsla av brådska eller erbjuder användaren något värdefullt. Det är viktigt att utbilda slutanvändarna att dubbelkolla att de kan lita på vem ett e-postmeddelande kommer från innan de klickar på länkar eller lämnar ut information. Även om det är omöjligt för användarna att fånga upp alla phishingmejl, kan säkerhetsmedvetenhet i kombination med skräppostfilter se till att den potentiella räckvidden för phishingmejl begränsas till ett minimum.

#2. Social Engineering

Phishing är bara en av många typer av social engineering-attacker. Fysiska och telefonbaserade social engineering-attacker används också av brottslingar för att få tillgång till säkra lokaler och känsliga uppgifter.

Det är viktigt att de anställda får utbildning om de olika typerna av social engineering - från de som sker via telefon till hot som sker personligen - och att de förstår hur de ska hantera en potentiell gärningsman på rätt sätt.

#3. Säkerhet hemma

Arbete hemifrån lyftes fram som en viktig fråga för slutanvändarnas säkerhet 2020, eftersom företag över hela världen uppmuntrade sin personal att byta till distansarbete. Den snabba övergången innebar att många användare lämnades dåligt utrustade med verktyg och kunskap för att säkerställa att de kan utföra sitt arbete på ett säkert sätt.

Det är viktigt att utbilda alla anställda som arbetar hemifrån om hur de kan se till att företagets data och nätverk inte äventyras genom fjärråtkomst. Uppdatering av programvara, skydd av Wi-Fi-nätverk och användning av säkerhetsverktyg som VPN för att garantera säker åtkomst har blivit en viktig del av utbildningen för slutanvändare.

#4. Säker användning av e-mail och internet

Det är sällsynt att en anställd inte använder internet eller e-post på jobbet. Pandemin har gjort företag mer beroende av internet än någonsin, men användningen av internet medför också säkerhetsrisker. Användare kan oavsiktligt installera skadlig kod, läcka uppgifter, lämna ut inloggningsuppgifter till phishingmejl eller falla för någon av de många andra attacker som cyberbrottslingar riktar in sig på dem. Det är viktigt att utbilda användarna i att använda internet och e-post på ett säkert sätt. Det handlar till stor del om medvetenhet: att veta att e-postmeddelanden kan orsaka dataintrång om de skickas ovarsamt och att skadliga webbplatser kan innehålla skadlig kod.

Det bör också finnas praktiska råd i utbildningen, t.ex. att informera användarna om skillnaden mellan cc- och bcc-fälten och vad HTTPS-krypteringssymbolen på webbplatser betyder.

#5. Arbeta på distans

Distansarbete kommer att bli populärare än någonsin. Även om pandemin har gett hemarbete en startpunkt i många företag, kommer det sannolikt att fortsätta efter pandemin. De anställda har börjat vänja sig vid att arbeta hemifrån och företagen inser fördelarna med detta.

Att arbeta på distans innebär också risker. Bärbara datorer, mobiltelefoner, surfplattor och andra enheter kan utgöra ett allvarligt säkerhetshot om de förloras eller stjäls. Om anställda lagrar eller får tillgång till företagsuppgifter från sina mobila enheter blir alla dessa uppgifter sårbara om en enhet hamnar i fel händer. När man utbildar användare om säkert distansarbete bör man fokusera på att hjälpa användarna att identifiera punkter där system eller data kan äventyras - och vilka åtgärder de kan vidta för att minska dessa risker.

#6. Mobila enheter

Användningen av mobila enheter i företag har ökat snabbt och trenden förväntas bli ännu mer utbredd än tidigare. Mobila enheter som bärbara datorer, mobiltelefoner och surfplattor gör det möjligt för de anställda att arbeta hemifrån, från kaféer, på resande fot eller nästan var de vill, vilket ger flexibilitet både för dem själva och för företaget. Även om mobila enheter är bekväma, så medför de risker som användarna måste utbildas om.

Användarna bör utbildas om hur mobila enheter potentiellt kan utsätta företagets data och system för obehörig åtkomst. Det handlar om åtkomst genom förlorade eller stulna enheter, samt skadlig programvara och olagliga appar från tredje part.

#7. Lösenord och autentisering

Lösenord fortsätter att vara ett problem för företag, anställda och kunder. Människor är helt enkelt inte konstruerade för att komma ihåg långa, komplexa fraser - särskilt inte dussintals fraser. Detta innebär att anställda ständigt frestas att ta den enkla vägen och göra dem lätta att komma ihåg - särskilt när de måste dela tillgång till appar och tjänster med sina kollegor.

Majoriteten av slutanvändarna är medvetna om varför det är viktigt med lösenordssäkerhet och har en grundläggande uppfattning om vad som kännetecknar ett starkt lösenord. Utbildningen om lösenord och autentisering bör fokusera på att ge praktiska råd om hur man kan upprätthålla lösenordssäkerheten utan att göra livet svårare för slutanvändarna. Detta innebär att uppmuntra användningen av lösenordshanterare (om det är något som ditt företag tillåter), be de anställda att aktivera tvåfaktorsautentisering för alla tjänster och system med tillgång till känsliga uppgifter, samt lära de anställda hur man skapar ett lösenord som både är någorlunda komplext och någorlunda lätt att komma ihåg.

#8. Säkerhet i molnet

Under de senaste åren har företagstjänster och data i allt högre grad flyttats över till molnet, och många verksamheter bedrivs helt och hållet med hjälp av webbaserade verktyg och tjänster. Även om molnet erbjuder stor flexibilitet för företag är det viktigt att användarna vet hur de ska använda och få tillgång till det på ett säkert sätt.

Starka lösenord och autentisering samt e-postsäkerhet blir extra viktigt när ditt företag använder molntjänster.

En cyberkriminell som gissar en anställds lösenord kan få tillgång till dina känsliga uppgifter från var som helst i världen, och därför är det viktigt att de anställda får utbildning om de åtgärder som krävs för att hålla molnkonton säkra. Flerfaktorsautentisering är särskilt viktigt för företag som hanterar känsliga uppgifter.

#9. Allmänt Wi-Fi

Eftersom användarna i allt större utsträckning arbetar när de är på språng är det troligt att de ansluter till företagstjänster, nätverk eller data från offentliga Wi-Fi-åtkomstpunkter. Offentligt Wi-Fi är mycket bekvämt för mobilt arbete, men innebär också säkerhetsrisker.

Det är viktigt att lära slutanvändarna att deras data potentiellt kan avlyssnas på offentliga Wi-Fi-nätverk. Om du tillåter dina slutanvändare att få tillgång till företagets data eller tjänster via offentliga Wi-Fi-nätverk bör du utrusta dem med programvara för virtuella privata nätverk och utbilda dem i hur man använder den på ett säkert sätt.

#10. Fysisk säkerhet

Även om hoten mot cybersäkerheten ökar är det viktigt att den fysiska säkerheten inte glöms bort. Det är ingen idé att skydda data med starka lösenord och flerfaktorsautentisering om en obehörig person helt enkelt kan gå in på kontoret och hämta en papperskopia av ett känsligt dokument direkt från skrivarfacket.

När slutanvändare utbildas i fysisk säkerhet är det viktigt att fokus läggs på att identifiera och minska hot som är relevanta för enskilda slutanvändares dagliga verksamhet. Om ditt företag är baserat på ett kontor kommer alla anställda att gå in genom kontorsdörren - så "tailgating" är ett exempel på ett säkerhetshot som är relevant för alla anställda.
Slutanvändarna bör utbildas i att aktivt tänka på vilka områden och dokument som är säkra, och se till att de alltid låses säkert eller redovisas när de inte används.

#11. Flyttbar media

Även om fildelning och samarbetstjänster på internet har blivit mer populära, används flyttbara enheter fortfarande i stor utsträckning i företag. Även om flyttbara enheter är användbara innebär de många risker: de kan lätt förloras eller stjälas, vilket kan leda till att data äventyras, eller så kan de ersättas med enheter som innehåller skadlig kod. En vanlig bluff är att lämna ett virusinfekterat USB-minne på en parkeringsplats på kontoret i väntan på att en intet ont anande anställd ska hämta det och sätta in det i en företagsdator. Dessutom är många användare omedvetna om att det inte bara är lagringsenheter som kan utgöra en risk: även enkla USB- eller laddningskablar kan modifieras av en cyberbrottsling så att de innehåller skadlig kod.

Att utbilda slutanvändare om säker användning av flyttbara medier handlar om ansvarstagande. Det bör klargöras för användarna att de måste ta ansvar för enheter som de har kontroll över - och att de inte ska koppla in enheter som inte har redovisats i någon dator, utan i stället rapportera dem till IT-teamet eller till säkerhetspersonal.

#12. Säker användning av sociala medier

Anställda - och företag - spenderar en allt större del av sin dag på sociala medier. Det är dock viktigt att se till att företagets säkerhet inte äventyras på grund av slarvig användning av sociala nätverk.

Fokus på utbildning i sociala medier bör ligga på att göra användarna medvetna om att det de delar med sig av kan vara tillgängligt för vem som helst på internet - och att även små detaljer från kontoret kan vara avgörande för angripare. En oskyldig selfie från kontoret kan till exempel visa en whiteboardtavla i bakgrunden med känslig företagsinformation eller till och med kunduppgifter.