IDENTIFIERING AV INFORMATIONSSÄKERHETSRISKER I VARDAGEN

Andreas Koschinski
EKM Service Ab Oy

INNEHÅLLSFÖRTEKNING

INLEDNING

Människor är ofta den svagaste länken i informationssäkerheten, men också den viktigaste. Genom att öka medvetenheten om säkerhetshot och följa bästa praxis kan företag hjälpa anställda att fatta välgrundade beslut som skyddar organisationens säkerhet.

Här är några andra anledningar till varför människor är den svagaste länken i säkerhet:

- Människor är ofta självsäkra och kan lätt bli lurade av cyberbrottslingar
- Människor följer inte nödvändigtvis bästa praxis för säkerhet.
- Människor kan klicka på skadliga länkar eller öppna bilagor från okända avsändare.

INLEDNING

Det är viktigt att komma ihåg att datasäkerhet är ett gemensamt ansvar. Företag måste vidta åtgärder för att skydda sina system och data, men anställda måste också vara medvetna om riskerna och vidta åtgärder för att skydda sig själva.

Genom att arbeta tillsammans kan vi alla bidra till att skydda våra länder och organisationer från cyberattacker.

NÄTFISKE

Phishing är inget nytt – det har varit den vanligaste attackvektorn för cyberbrottslingar i många år

Men i och med den ökande komplexiteten i nätfiskebedrägerier är det viktigare än någonsin att identifiera nätfiske.

MEN VAD ÄR PHISHING?

Ett nätfiskemeddelande är ett meddelande som ser ut att komma från en betrodd källa, men som i själva verket har skickats av en hotaktör med skadliga avsikter.

Phishing-epostmeddelanden kan skickas via e-post, webbplatser, textmeddelanden eller till och med sociala medier. Dessa meddelanden är ofta utformade för att se ut som äkta kommunikation från banker, myndigheter, nätverksleverantörer eller andra organisationer.

ATT KÄNNA IGEN NÄTFISKE DEL 1

- E-postmeddelanden som kräver brådskande åtgärder

E-postmeddelanden som hotar med negativa konsekvenser eller en missad möjlighet om inte brådskande åtgärder vidtas är ofta nätfiskemejl. Angripare använder ofta den här metoden för att stressa mottagarna innan de har haft en chans att undersöka e-postmeddelandet ytterligare.

- E-postmeddelanden med dålig grammatik och felstavningar

Ett annat sätt att identifiera nätfiske via e-post är dålig grammatik och felstavningar. Språkfel indikerar att en automatisk översättare har använts för att skriva meddelandet. Tyvärr gör tillkomsten av AI-program det svårt att identifiera hot enbart på grundval av språk. Eftersom ChatGPT och Co-pilot, till exempel, översätter text mycket bättre än gamla, traditionella textöversättare.

- E-postmeddelanden med en obekant hälsning eller ”styltiga” fraser

Medarbetare brukar använda informella hälsningar till varandra. Meddelanden som börjar med ”Ärade" eller ”Herr/Fru” samt innehåller fraser som vanligtvis inte används i en "informell" konversation kommer från källor som inte är bekanta med ditt företag och dina anställda. Meddelande som dessa bör misstänkas och behandlas därefter.

DEL 2

Inkonsekvenser i e-postadresser, länkar och domäner

Ett annat sätt att upptäcka nätfiske är att leta efter inkonsekvenser i e-postadresser, länkar och domäner. Kommer e-postmeddelandet från en organisation som det ofta finns korrespondens med? Kontrollera om länken är äkta genom att hålla muspekaren över länken för att se vad som kommer upp. Om e-postmeddelandet påstås komma (låt oss säga) från Google, men domänen ser ut som något annat, bör du rapportera e-postmeddelandet som en nätfiskeattack.

Suspekta bilagor

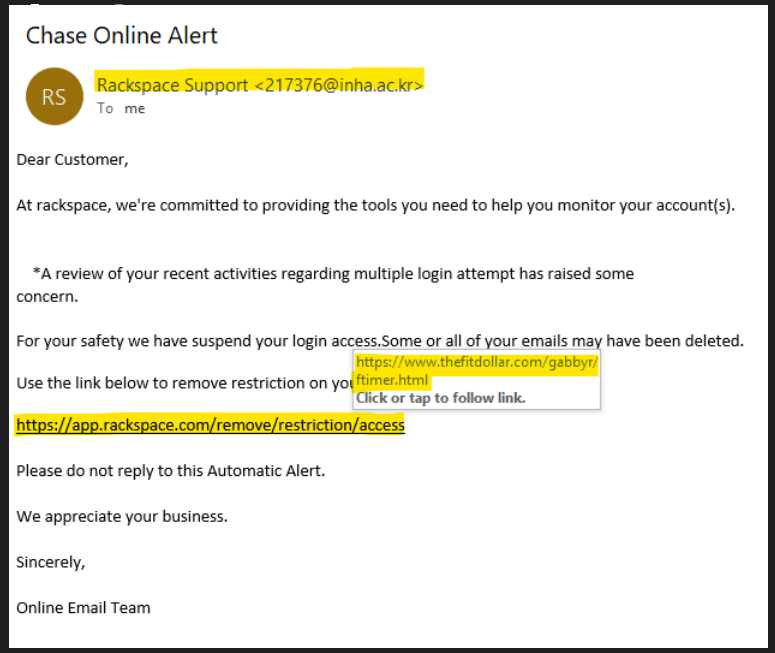
De flesta arbetsrelaterade fildelningar sker nu via samarbetsverktyg som SharePoint, OneDrive eller Dropbox. Därför bör interna e-postmeddelanden, eller ett oförutbestämt meddelande från en extern aktör med bilagor, alltid behandlas med misstänksamhet – särskilt om de har ett okänt filtillägg eller ett som vanligtvis förknippas med skadlig kod (.zip, .exe, .scr osv.).

E-postmeddelanden som begär inloggningar, betalningsinformation eller känsliga uppgifter

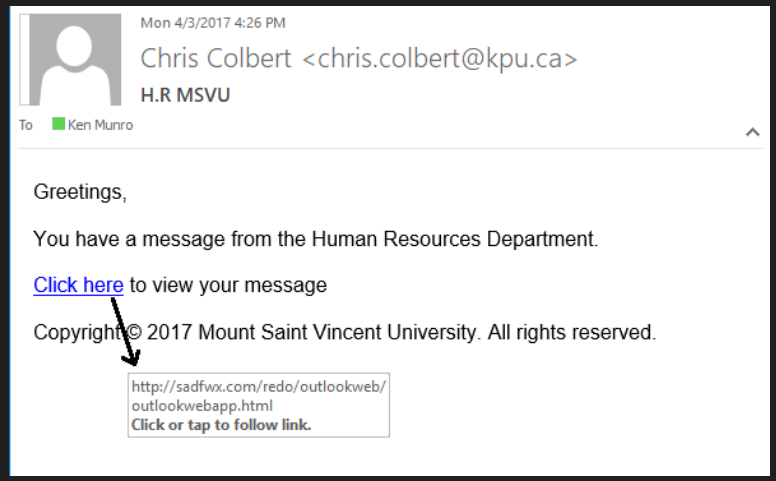
E-postmeddelanden från oväntade eller okända källor som begär inloggningsinformation, betalningsinformation eller annan känslig information bör alltid hanteras med försiktighet. Phishing-bedragare kan fejka inloggningssidor så att de ser ut som riktiga och skicka ett e-postmeddelande med en länk till en falsk sida. Alltid då mottagaren omdirigeras till inloggningssidan eller får veta att en betalning förfaller, bör de avstå från att ange information om de inte är 100 % säkra på att e-postmeddelandet är äkta och betalningen har överenskommits i förväg.

EXEMPEL I BILDER

Felaktigt framställd avsändare och förvrängd



"maskerad" länk



TILLFÖRLITLIGA NÄTVERKSADRESSER

Farliga länkar tar dig till farliga webbplatser och utsätter din data, din dator och dina nätverk för fara.

Även om det kan vara svårt att skilja en säker URL från en skadlig, finns det varningstecken man kan följa.

OSÄKER WEBBADRESS?

Alla webbadresser är inte likadana. Skadliga webbadresser lurar i e-postmeddelanden, textmeddelanden, inlägg på sociala medier, popup-fönster och mer.

Bedragare skapar och sprider dessa länkar och försöker locka användare som du att klicka på dem. När du landar på deras webbplatser kan du utsättas för skadlig programvara, virus, nätfiske och annat farligt innehåll.

HUR MAN IDENTIFIERAR EN WEBBADRESS - DEL 1

- Slutet av domänen är det viktigaste.

Domändelen av URL:en ger dig en uppfattning om källan till länken. Domännamnet kan hittas efter http://-delen. Domännamnet eller adressen slutar framför det **första** / tecknet. I länken http://google.com/maps är domänen till exempel google.com.

Verkar enkelt, eller hur? FEL.

Bedragare ändrar domäner för att få dem att se säkra ut. Till exempel, i länken http://google.com.cust_login.ie/, är domännamnet cust_login.ie, inte google.com. Och på länken http://accounts_login.cz/google.com är domänen accounts_login.cz, inte google.com.

Det här exemplet visar varför en användare kan tro att en länk leder dig till en Google-webbplats i stället för en skadlig webbplats. Därför är det viktigt att kontrollera statusen mellan http://-merkin och det första / tecknet och vara uppmärksam om något ser misstänkt ut.

- Viivat ja symbolit ovat yleisiä haitallisissa linkeissä.

Legitima webbplatser innehåller oftast inte bindestreck eller symboler i sina domäner. Som i exemplen som nämns ovan (_) använder bedragare dessa element tillsammans med välkända varumärken i ett försök att lura dig. Till exempel är www.google.com inte samma sak som www.google-search.com.

DEL 2

- Var helt försiktig med numeriska domäner.

Ibland kan du stöta på en domän som bara visas som en IP-adress (t.ex. http://101.10.1.101). I sådana länkar vet du inte den verkliga ägaren till webbplatsen. Du bör inte klicka på en sådan URL om du inte känner till IP-adressens ursprung och vet exakt vart adressen kommer att gå.

- Förkortade webbadresser är maskering av webbadresser. Punkt.

Vissa sociala medieplattformar har teckenbegränsningar, så det är vanligt att se förkortade webbadresser på dem. De kan också hittas i textmeddelanden, e-postmeddelanden och andra medier. Tjänster som Tiny URL och Bitly tar längre webbadresser och kombinerar dem med kortare webbadresser. Även om detta är bekvämt, är den förkortade URL:en i verkligheten en mask för en annan länk. Var försiktig med dessa; Precis som med IP-adressdomäner kan du inte vara säker på de faktiska källorna till länkarna. T.ex. https://bit.ly/3Bg19uM kan leda vart som helst.

- Bedragare maskerar farliga länkar som legitima länkar.

Bedragare kan bädda in farliga webbadresser i länkar, text, logotyper och bilder som ser legitima ut. Men du kan se vad som är dolt när du håller muspekaren över dessa länkar. Jämför webbadressen på skärmen med det som är synligt. Om det finns betydande skillnader eller om du ser några varningstecken i den dolda URL:en ska du undvika länken (och e-postmeddelandet, webbplatsen eller annonsen som innehåller den).

LÖSENORDSSÄKERHET

Lösenord är nyckeln till nästan allt du gör online, och du har förmodligen flera lösenord som du använder under dagen.

Att välja starka lösenord som är svåra att knäcka och hantera dem på ett säkert sätt kan ibland kännas omständigt. Lyckligtvis finns det enkla sätt att göra dina lösenord så säkra som möjligt.

LÖSENORDSSÄKERHET DEL 1

- Avslöja aldrig dina lösenord för andra.

Du skulle förmodligen inte ge ditt betalkort och din PIN-kod till en främling. Så varför ange ditt användarnamn och lösenord? Dina inloggningsuppgifter skyddar information som är lika värdefull som dina pengar på ditt bankkonto. Ingen annan än du behöver dem – inte ens IT-avdelningen. Om någon ber om ditt lösenord är det en bluff.

- Använd olika lösenord för olika konton.

Således, om ett konto äventyras, är de andra fortfarande säkra.

- Käytä monivaiheista tunnistautumista (MFA).

Även de bästa lösenorden har sina gränser. Multifaktorautentisering lägger till ytterligare ett lager av säkerhet utöver ditt användarnamn och lösenord. Vanligtvis är en ytterligare faktor ett sms eller en mobiltelefonapp du använder för att bekräfta att du faktiskt försöker logga in.

- Längd övervinner komplexitet.

Ju längre lösenordet är, desto bättre är det. Använd minst 12 tecken när det är möjligt. Komplexitet är fortfarande viktigt. Om du vill göra det ännu mer komplicerat kan du använda versaler och gemener, siffror och specialtecken. Lösenordet bör använda minst 3 av dessa alternativ.

DEL 2

- Gör dina lösenord svåra att gissa men lätta att komma ihåg.

Om du vill göra lösenord lättare att komma ihåg kan du använda fraser eller uttryck. Till exempel ”smörgåsochskinkanam". I vissa system kan du till och med använda mellanslag: "smörgås och skinka nam".

Undvik enstaka ord eller ord som följs eller föregås av en enda siffra (t.ex. Lösenord1). Hackare använder ordböcker och vanliga lösenord för att gissa ditt lösenord.

Använd inte information i ditt lösenord som andra kan känna till om dig eller som finns på dina sociala medier (t.ex. födelsedagar, namn på barn eller husdjur, bilmodell etc.). Om dina vänner kan hitta det kan hackare också göra det.

Ju längre lösenordet är, desto bättre är det. Använd minst 12 tecken när det är möjligt. Komplexitet är fortfarande viktigt. Om du vill göra det ännu mer komplicerat kan du använda versaler och gemener, siffror och specialtecken. Lösenordet bör använda minst 3 av dessa alternativ.

För att göra det tidigare exemplet ännu säkrare: "Smörgås&skinkaNAM!".

How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

Number of Characters	Lowercase Letters Only	At Least One Uppercase Letter	At Lease One Uppercase Letter + Number	At Lease One Uppercase Letter + Number + Symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 minutes	6 minutes
8	Instantly	22 minutes	1 hour	8 hours
9	2 minutes	19 hours	3 days	3 weeks
10	1 hour	1 month	7 months	5 years
11	1 day	5 years	41 years	400 years
12	3 weeks	300 years	2,000 years	34,000 years

Source: Security.org

TACK!

Andreas Koschinski
0500 486 091
ak@ekm.fi
www.ekm.fi