OUCH!

SANS SECURITY AWARENESS

Det månatliga nyhetsbrevet om säkerhetsmedvetenhet till dig!

Fyra enkla steg som håller dig säker

Översikt

Att utnyttja tekniken på ett tryggt och säkert sätt kan verka överväldigande och förvirrande. Här är fyra enkla steg som hjälper dig att vara säker oavsett vilken teknik du använder eller hur du använder den.

1. Du: Först och främst, endast teknik kan inte skydda dig, du är ditt bästa försvar. En angripare har lärt sig att det enklaste sättet att få vad de vill är att attackera dig i stället för din dator eller dina andra enheter. Om de vill ha ditt lösenord, kreditkort eller kontroll över din dator kommer de att försöka lura dig att ge bort det, ofta genom att skapa en känsla av att det är brådskande. Till exempel kan de låtsas ringa från Microsofts tekniska support och hävda att din dator är infekterad men i själva verket är de bara cyberbrottslingar som vill få tillgång till din dator. Eller kanske skickar de en varning med e-post att ditt paket inte kunde levereras och att du måste klicka på en länk och bekräfta din e-postadress, när de i verkligheten lurar dig att besöka en skadlig webbplats som hackar din dator. I slutändan är du det bästa försvaret mot angripare.Med sunt förnuft kan du upptäcka och stoppa många attacker.

2. Lösenordsfraser: Moderna och kraftfulla datorer har gjort det gamla lösenordet med 8 tecken föråldrat och sårbart. När en webbplats ber dig skapa ett lösenord skapar du istället en stark och unik lösenordsfras. En lösenordsfras är en typ av lösenord som använder en serie ord som är lätt att komma ihåg, till exempel “ bi honung bourbon regn. “Ju längre din lösenordsfras är, desto starkare är den. En unik lösenordsfras betyder att man använder olika lösenord för varje enhet eller online- konto. Med den här metoden är alla dina andra konton och enheter fortfarande säkra om din lösenordsfras blir komprometterad. Kommer du inte ihåg alla lösenordsfraser? Använd en lösenordshanterare som är ett speciellt program som lagrar alla dina lösenordsfraser krypterat och säkert (och har också en mängd andra användbara funktioner).

Slutligen, aktivera tvåstegsverifiering (även kallad tvåfaktors- eller flerfaktorsautentisering). Det använder ditt lösenord, men lägger också till ett extra steg, till exempel skickas en kod till din smarta telefon eller använd

en app som genererar koden åt dig. Tvåstegsverifiering är förmodligen det viktigaste steget du kan ta för att skydda dina online- konton och det är mycket lättare än du kanske tror.

3. Uppdatering: Se till att alla dina datorer, mobila enheter, program och appar kör den senaste versionen av sin programvara. Cyberangripare letar ständigt efter nya sårbarheter i den programvara som dina enheter använder. När de upptäcker sårbarheter använder de speciella program för att utnyttja dessa och hacka dina enheter. Samtidigt arbetar företagen som utvecklade programvaran hårt med att fixa dessa och släppa uppdateringar. Genom att se till att dina datorer och mobila enheter installerar dessa uppdateringar snabbt gör du det mycket svårare för någon att hacka dig. Håll dig uppdaterad genom att aktivera automatisk uppdatering där det är möjligt. Denna regel gäller nästan all teknik som är ansluten till ett nätverk, inklusive internetansluten TV, babymonitorer, säkerhetskameror, hemroutrar, spelkonsoler eller till och med din bil.

4. Säkerhetskopiering och återställning: Ibland, oavsett hur försiktig du är, kan du bli hackad. Om så är fallet kan "återställa säkerhetskopior" vara det enda sättet att få tillbaka din personliga information. Se till att du gör regelbundna säkerhetskopior av viktig information och kontrollera att du kan återställa data från dem. De flesta operativsystem och mobila enheter stöder automatiska säkerhetskopior, antingen till externa enheter eller till molnet.

Gästredaktör

*SANS Certifierad instruktören **Steve Anson** ger vägledning till IT-säkerhetsteam och regeringar runt om i världen för att förbättra deras säkerhetsförmåga. Steve är författaren till den kommande boken Applied Incident Response och tillhandahåller gratis råd för IT-säkerhetsutövare på www.AppliedIncidentResponse.com.*

Referenser

Social Engineering: https://www.sans.org/u/W3G
Personalized Scams: https://www.sans.org/u/W3Q
Making Passwords Simple: https://www.sans.org/u/W3V
Got Backups: https://www.sans.org/u/W40

OUCH! Publiceras av SANS Security Awareness och distribueras under Creative Commons BY-NC-ND 4.0-licens. Du kan fritt distribuera nyhetsbrevet eller använda det i ditt medvetenhetsprogram så länge du inte ändrar innehållet i nyhetsbrevet. För översättning eller mer information, vänligen kontakta www.sans.org/security-awareness/ouch-newsletter. Redaktion: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Översatt av: Johan Ahlberg