5 SÄTT
SOM DU INTE KÄNDE TILL ATT DU KUNDE FÅ ETT VIRUS, MALWARE ELLER ATT DITT SOCIALA KONTO KUNDE HACKAS

De flesta tekniskt kunniga personer är bekanta med standardformerna av malware: nätfiske, reklamprogram, spionprogram, virus, maskar och liknande. Men i takt med att tekniken utvecklas gör webbbrottslingarna också det, och de letar hela tiden efter dolda sätt att få tag på din information. Detta resulterar i att det finns nya former av malware som du kanske inte känner till.

BEDRÄGERIER OCH MALWARE I SOCIALA MEDIER

Grayware är en form av malware som inte gör någon fysisk skada på dina data som andra skadliga program kan göra. Den visar sig på ett mer irriterande sätt, till exempel i form av reklamprogram och spionprogram. Den har hög förekomst i sociala medier, vanligtvis i form av ”klickbete”, där en lockande artikel leder dig till en webbplats där du uppmanas att fylla i en snabb undersökning innan du kommer åt medierna. Den informationen samlas sedan in och säljs till andra webbrottslingar, och den kan användas i försök att hacka dina personliga konton. Om du vill veta mer om hur du skyddar dig mot dessa typer av bedrägerier kan du även läsa artikeln ”Social media scams based on current events” som finns på Norton.com för att lära dig mer om sociala bedrägerier.

Förutom att grayware löper amok på dessa plattformar finns det även stora risker för att stöta på farlig malware på sociala nätverk. När TV-showen ”Breaking Bad” var som mest i ropet fanns det en populär Twitter-bluff i faggorna. Länkar lades upp för att locka användare att ladda ner en läckt kopia av nästa avsnitt som ännu inte hade sänts. Om man följde länken kom man till en sida där en fil laddades ner. Sedan fördes användarna till en annan länk för att installera ett program som skulle göra det möjligt för dem att spela upp videon. Länken skickade användarna till ett associerat program, och det var så spammarna tjänade pengar. Denna bluff verkade ganska ofarlig för användarens dator, men det finns andra fall där det som laddas ner är ett farligt malwareprogram. Var alltid försiktig när du klickar på okända länkar och försöker ladda ner okända filer.

UTNYTTJANDEPAKET

Utnyttjandepaket är i allmänhet precis som det låter – ett skadligt verktygskit som söker igenom din dator efter programvara som inte har uppdaterats. Dessa kit söker efter säkerhetsluckor i programvara med målet att lägga in malware på användarens enheter. Detta kan hända när man besöker webbplatser som har malvertising. Malvertising kan finnas på alla webbplatser, betrodda eller okända, och använder onlineannonsering genom att bädda in skadlig kod i legitima annonser. Nyligen var Yahoo ett mål för detta genom att vara värd för skadliga annonser som omdirigerade användare till webbplatser som hade dessa paket. Men utnyttjandepaket finns inte bara i malvertising. Den populära webbplatsen för män Askmen.com kompromitterades nyligen vilket innebar att användare omdirigerades till en webbplats som hade ett utnyttjandepaket. Därför är det mycket viktigt att du ser till att all programvara är uppdaterad.

UTPRESSNINGSPROGRAM PÅ MOBILER

Utpressningsprogram på datorer är inget nytt hot, men nyligen har det börjat migrera till populära mobila plattformar. Utpressningsprogram är ett program som riktar in sig på viktiga filer som foton och dokument, och krypterar dem och blockerar användaren från att komma åt dem. Användaren får sedan ett meddelande med krav på betalning för att låsa upp filerna. Tidigare i år upptäcktes de första versionerna av utpressningsprogram på mobiler. Man kan utsättas för utpressningsprogrammet genom att besöka en infekterad webbplats, och sedan laddas det ner automatiskt till mobilen eller genom att man laddar ner en skadlig app. Om din enhet blir smittad, betala inte avgiften! Se istället till att du skaffar dig vanan att regelbundet säkerhetskopiera och återställa mobilen från den senaste säkerhetskopian. Du kan lära dig hur man upptäcker falska mobilappar genom att kolla in ”How to Spot a Fake Android App” på Norton.com.

MALWAREANGREPP VIA ONLINESPEL

Det har förekommit några fall av spelmalware i media på sistone. Detta kanske inte kostar dig pengar, men det kan kosta dig de många timmar du har lagt ner på att bygga upp dina karaktärer. Twitch.tv, en webbplats som används för att streama livespel, infiltrerades nyligen av en robot i deras chattrum som lockade användare med hjälp av utlottningar. När du klickar på länken för att komma till utlottningen visar en Java-form ett falskt utlottningsformulär. När formuläret har fyllts i installerar malware sig på användarens dator, riktar in sig på användarens Steam-konto och tömmer sedan hela Steam-plånboken och innehållet. Sedan kan webbrottslingarna sälja användarens artiklar på Steam-forumet. På samma sätt fanns det ett problem med en illvillig trojan i det populära spelet World of Warcraft, maskerad till ett legitimt speltillägg. När trojanen har installerats tar den över användarens konto helt. Vi rekommenderar att användare inte inaktiverar sina antivirusprogram när de spelar onlinespel.

REKLAMPROGRAM OCH MALWARE I WEBBLÄSARTILLÄGG

Webbläsartillägg är mycket populära tillägg som används till en mängd uppgifter medan du surfar på internet. Men du är säkert inte medveten om att några av dem kan stjäla din information! Vissa skadliga tillägg kan antingen spåra alla webbplatser du besöker eller lägga in reklamprogram på dessa webbplatser. Även om detta inte är något stort bekymmer när det gäller information på din dator, är det ett ganska stort integritetsproblem. Angripare kan använda dessa tillägg för klickbedrägeri genom att lägga till oseriösa annonser på webbplatser och omdirigera dig till dessa webbplatser. Även om detta ligger lägre på hotnivån, utvecklas denna nyare form av malware till något mycket mer invasivt. Faktum är att Europeiska unionens byrå för nät- och informationssäkerhet (ENISA) har varnat för ökningen av skadliga webbläsartillägg som försöker ta över sociala nätverkskonton. Även om de för tillfället inte är överst på hotlistan är de definitivt något att hålla koll på.

Internethot kan förekomma i alla former och storlekar, och det kan vara många du kanske inte känner till. Vi skyddar dig så att du inte behöver oroa dig för varje liten sak du kan stöta på. Du kan göra det du ska och lämna de komplicerade sakerna till oss.