Varför måste mitt barn vara rädd om sina nätkonton?

> Kapade konton i sociala medier och onlinespel kan missbrukas för bedrägerier och nätmobbning.

> Prata med ditt barn om att lösenord är värdehandlingar som inte ska delas med vänner eller lämnas ut hur som helst.

> Ett tips för att skydda konton är att aktivera tvåfaktorsautentisering.

Läs mer: www.statensmedierad.se

Det långa svaret

Varför är ett kapat konto värdefullt för bedragare?

Att inloggningsuppgifterna till ett bankkonto är viktiga att skydda förstår vi instinktivt, eftersom där finns pengar som kan stjälas. Att andra konton, som de i sociala medier och onlinespel, är värdefulla är inte lika uppenbart. Men också här finns sånt som intresserar kriminella och andra:

- I en del onlinespel finns spelvalutor som används för att köpa innehåll i spelen och som därmed har ett ekonomiskt värde.
- Ett kapat konto med många följare eller som på annat sätt är värdefullt för innehavaren kan användas för utpressning.
- Ett kapat konto kan också användas för att posta innehåll och kommentarer i den drabbades namn, och få hen att framstå i dålig dager.
- Listan med kontakter är en bra startpunkt för den som vill försöka genomföra nätbedrägerier.

> Om en främmande person ber någon överföra pengar eller låna ut sina engångskoder till bankkontot skulle de flesta av oss säga nej direkt. Men om frågan kommer från klasskompisen eller kollegan?”

De tre första punkterna är självförklarande. Men varför är de som vill begå bedrägerier också intresserade av att kapa konton på nätet? Jo, det sänker garden hos den som utsätts för bedrägeriförsöket. Om en främmande person ber någon överföra pengar eller låna ut sina engångskoder till bankkontot skulle de flesta av oss säga nej direkt. Men om frågan kommer från klasskompisen eller kollegan? Då är det lätt hänt att man vill vara en bra kompis och hjälpa till.

Att se över säkerheten för sina konton på nätet är alltså inte bara ett sätt att skydda sig själv, utan också ett sätt att minska risken för att kompisarna blir lurade. Den här typen av bedrägerier kallas ibland för Facebook-bedrägerier, eftersom det är vanligt

att de sker från kapade Facebook-konton. Men de är inte begränsade till den plattformen. Tvärtom kan de genomföras från alla plattformar där det går att skicka personliga meddelanden mellan användare.

Swedbank producerade några år sedan en film som visar hur ett Facebook-bedrägeri kan genomföras.

Undvik att bli utsatt för nätfiske (phishing)

Ett sätt att lura av användare deras inloggningsuppgifter är genom löften om gratis spelvaluta, att deras konto ska bli ”verifierat” (en blå liten ikon som läggs till profilbilden på bland annat Instagram och Twitter för att visa att kontot tillhör personen det påstås tillhöra) eller något annat som är eftertraktat på den aktuella plattformen.

Ett sätt att lura av användare deras inloggningsuppgifter är genom löften om gratis spelvaluta

För att löftet ska kunna infrias behöver användaren först skicka sina inloggningsuppgifter. Detta kan bland annat ske via fejkade webbsidor, som vid första anblicken kan se ut som exempelvis en officiell Instagramsida. Det här är samma tillvägagångssätt som de bedragare som försöker komma över inloggningsuppgifter till bankkonton också använder sig av. Tekniken kallas för phishing.

Också offentliga institutioner som Socialstyrelsen, Folkhälsomyndigheten och sjukvården används som falska avsändare. Det ditt barn behöver lära sig är att ingen med ärligt uppsåt kommer att be om inloggningsuppgifter på det här sättet.

Lämna inte ut engångskoder

Swedbanks film visar inte bara hur ett kapat konto används för att lura en intet ont anande person. Killen i filmen har inte heller förstått hur engångskoder fungerar. En engångskod är, precis som ett BankID, ett extra skydd till ett konto. Finessen med de tekniska lösningarna är att de ger ett extra skydd när pengar ska överföras mellan konton, när en räkning ska betalas eller när man ska logga in på ett konto i sociala medier.

För den typen av transaktioner räcker det inte med lösenordet. Anledningen är att lösenord kan stjälas, gissas eller komma på avvägar på andra sätt. Genom att komplettera lösenordet med en kod som skapas från exempelvis en bankdosa får kontot ett extra skydd. Det räcker då inte längre med ett lösenord för att kunna stjäla pengar, man måste också ha koden.

Men varje konto har sina egna engångskoder. De koder som kan användas för att bekräfta en överföring från ditt bankkonto kan därför inte användas för att betala räkningar från någon annans. Därför ska du säga åt ditt barn att aldrig lämna ut engångskoder till någon annan, inte ens när bästa kompisen ber om den. Koden kan bara användas för att logga in på ditt barns konto och vill någon annan ha engångskoderna är det något misstänkt på gång.

Skydda konton med engångskoder

Det vanligaste är att man kommer i kontakt med engångskoder som hör till bankkontot, men det är inte det enda stället på nätet där den funktionen finns. Facebook, Instagram och Snapchat är exempel på sociala medier där det går att ge sina konton extra skydd genom engångskoder, eller tvåfaktorsautentisering som det också kallas. Ofta förkortat 2FA.

I spelvärlden finns 2FA bland annat på Fortnite, på Steam och på Twitch. Ett Google-konto, och därmed också ett Youtube-konto, går att skydda på samma sätt. På webbplatsen Two Factor Auth finns en lång lista med sajter och tjänster där det går att aktivera tvåfaktorsinloggning.

Om ni bestämmer er för att aktivera engångskoder, vilket är en bra idé, är det också viktigt att läsa på ordentligt hur de fungerar på de tjänster ni använder. Om tjänsten exempelvis skickar engångskoderna via sms till en mobiltelefon, kolla vad som händer om man byter mobilnummer men glömmer att ändra inställningarna. Det finns en risk att man av misstag råkar låsa sig ute från sina egna konton. Men alla tjänster har med det i beräkningen och olika sätt att minimera den risken. Så, läs på.

Vad är ett säkert lösenord?

> Det första ditt barn behöver förstå är att lösenord är värdehandlingar som inte ska delas med kompisar.”

Över hela den här diskussionen svävar frågan om lösenord. Det första ditt barn behöver förstå är att lösenord är värdehandlingar som inte ska delas med kompisar. Det andra är vad som kännetecknar ett säkert lösenord: Det ska vara någorlunda långt, åtminstone åtta tecken, och inte ett ord som är lätt att gissa. Det ska heller inte vara något av de lösenord som finns med på listor över de allra vanligaste lösenorden.

Tipsruta

- Prata med ditt barn om varför lösenord är värdehandlingar och varför fler konton än bankkonton är värda att skydda.
- Berätta för ditt barn varför inloggningsuppgifter aldrig ska lämnas ut när någon frågar efter dem och att ingen annan, inte ens bästa kompisen, har någon som helst användning av ditt barns engångskoder.
- Sätt dig tillsammans med ditt barn och aktivera engångskoder på de konton där det är möjligt.

Källa:

Facebook.
Fortnite.
Google.
Instagram.
Karasek, J. och Pernet, C. (2019) *How a Hacking Group is Stealing Popular Instagram Profiles.* Trend Micro.
Snapchat.
Steam.
Swedbank.
Twitch.
Two Factor Auth.
1177 Vårdguiden.
Wikipedia.org.