Privata funderingar kring kapning av ett MS konto

Reviderat 2020-05-23

Om oturen skulle vara framme – En jämförelse.

Att **inte kunna logga in på sitt konto** kan jämföras med att **inte komma in i sitt hem.**

I båda fallen gäller det att ha tänkt igenom situationen **i förväg** och **förberett sig** för den.

> Man har **glömt/tappat nyckeln** – Kan enkelt lösas om det finns reservnyckel att tillgå. Som att **återställa lösenordet**.
>
> **Saknas reservnyckel** eller har **någon har bytt ut låset** och inte gett dig en ny nyckel – Kräver betydligt större insats för att återta lägenheten och eventuellt byta ut låset igen. Du måste bevisa för låssmeden/polisen att du är du och att hemmet är ditt. Som att **återställa kontot.**
>
> När du återställer kontot tas de gamla verifieringsuppgifterna bort och du måste ange ny (om än tillfällig) e-postadress, som inte fanns knutet till kontot tidigare. Ny återställningskod genereras och tvåstegs verifiering måste aktiveras på nytt. När du väl kommit in på kontot igen kan du lägga tillbaka dina gamla verifieringsuppgifter.

Bedragarens motiv o mål

Målet kan vara att ta över ditt konto genom din inloggning för att göra något av följande.

A. Stjäla dina mejlkontakter och använda dem i sitt eget syfte
   a. Väl inne i din e-post görs förändringar som påverkar distributionen av din egen mejl som omdirigeras någonstans.
   b. Du lär inte märka något förrän dina kontakter regerar eller att du märker att du slutat få post.

B. Ställa om kontot så att du själv inte kan använda det, bara för att sabotera eller för att kunna jobba ostört i din miljö
   a. Du kan inte logga in, varken på kontot eller på din mejl.

Tänkbara tillvägagångssätt för bedragaren att komma över dina uppgifter

- Försöka hacka ditt konto på egen hand.
- Köpa dem av annan hacker.
- Använda Nätfiske för att lura av dig dem. Se artikel om ”spoofing”
- Ringa dig och utge sig vara från Microsoft för att ”återställa din dator som man ser har problem”. Sker inte sällan på knackig engelska.
- Använda sig av virus i form av ”trojan” som när den är på plats på din dator kan skicka information till bedragaren. En s.k. ”keylogger” är ett exempel på detta.
- Använda 2-stegs verifieringen i sitt eget syfte genom att lyckas stjäla mobilnumret. Se vidare under Finns det bister …

Hur kan du påverkas när kontot väl är kapat och dina uppgifter ändrade

- Alla funktioner som kräver inloggning upphör att fungera
- Inloggning på din egen enhet om du på den har endast ett konto som tillika bygger på din e-postadress.
- Inloggning på ditt konto via internet.
- Inloggning på din mejl.
- Inloggning på Skype.
- Inloggning på MS tjänster över huvud taget.

Hur kan du förhindra/ försvåra ett övertagande?

Använd svårforcerade lösenord: Utnyttja versaler, gemener, siffror och specialtecken i kombination.

Komplettera kontot med uppgifter för verifiering vid inloggning och vid återställning av lösenord**,** i form av telefonnummer och alternativ e-post adress. Använd gärna ett konto hos Gmail men inte någon domän som är knuten till din anställning eller boendeform eftersom dessa kan ändras då du slutar ditt jobb eller byter bostad.

Komplettera med att skapa en återställningskod som kan användas för att återställa / återta kontot.

Tvåstegs verifiering kräver ett extra moment om ditt konto loggar in på annan enhet än din egen, alltså även om kaparen har din inloggning. Antar att detta kan resultera i att kontot låses, under begränsad tid men det ger dig i alla fall en möjlighet att återta kontrollen om än inte på en gång. Se vidare under Finns det bister …

Lägg in alias på kontot som kan användas till att lämna ut till någon som du inte känner/ litar på. Alias kan användas för att skicka mejl till dig men går inte att användas för kontoinloggning om man anger det.

Finns det brister i/nackdelar med 2-stegsverifiering?

På senare tid har det visat sig att det finns kryphål, i synnerhet om man använder mobilen för att få verifieringskod via sms.

Tvåstegsverifiering (2SV) lägger ett lager av säkerhet till MS kontot. Först anger man sitt lösenord och blir därefter tvungen att lägga till en extra kod som man får vi sms eller mejl. Detta innebär att en hackare skulle behöva stjäla både lösenord och telefon för att bryta sig in på kontot.

Hackare har kunnat lura teleoperatörer att överföra ett telefonnummer till en ny enhet ett s.k. SIM-byte. Detta förutsätter vanligen att bedragaren också skaffat sig en del annan information. När väl det är gjort går begäran om sms kod till honom. Den egna telefonen blir obrukbar.

Sedan finns det svagheterna i själva mobiltelefonsystemet. I det som kallas en SS7-attack kan en hackare spionera via mobiltelefonsystemet, lyssna på samtal, fånga textmeddelanden och se platsen för din telefon.

Vad kan man använda istället?

I säkerhetsinställningarna för kontot kan man välja om kod skall skickas via mobil (sms), fast telefon (sms eller bli uppringd) eller extra mejlkonto. Valet är upp till användaren.

Referensmaterial

Säkerhetsinformation: https://support.microsoft.com/sv-se/help/12428

Kan inte logga in: https://support.microsoft.com/sv-se/help/12429

Kontot är låst: https://support.microsoft.com/sv-se/help/13956

Ovanlig inloggnings aktivitet: https://support.microsoft.com/sv-se/help/13967/microsoft-account-unusual-sign-in

Kontot är hackat: https://support.office.com/sv-se/article/mitt-outlook-com-konto-har-hackats-35993ac5-ac2f-494e-aacb-5232dda453d8

En bloggartikel om att bli hackad: https://it-bloggen.com/284-sa-blir-du-hackad-och-sa-undviker-du-det

En webbsiteartikel om spoofing: https://lifehacker.com/how-spammers-spoof-your-email-address-and-how-to-prote-1579478914

Häva blockering av konto: https://support.office.com/sv-se/article/ta-bort-blockering-av-mitt-outlook-com-konto-f4ad2701-d166-4d8b-8a6a-9af2a1f8a4c4

Återställa konto: https://support.microsoft.com/sv-se/help/17875/microsoft-account-reset-or-recover-password

Kontohjälp via e-post: https://support.microsoft.com/sv-se/help/12401/microsoft-account-get-help-by-email