IT-säkerhet
för moderater

nya MODERATERNA

Innehåll

Sid

Visa omdöme i din digitala kommunikation **4**

Skydda dig mot intrång och ”phising” **5**

Åtgärder för att minska risken för att bli utsatt för bedrägerier och ID-kapning **10**

Ta säkerhetskopior **11**

Använd kryptering och bra lösenord på telefon och dator **12**

Ytterligare verktyg för att höja din säkerhet **13**

Hot och trakasserier på nätet **15**

Förord

Under valen i USA och Frankrike påverkades politiska partier negativt av attacker på deras it-system. Vi moderater har bestämt oss för att reducera risken för att samma sak händer oss och skärper därför vår egen IT-säkerhet. Vi gör det inte bara för att skydda oss själva utan också för att skydda den svenska demokratin.

IT-säkerhet var tills för inte så länge sedan något som enbart IT-experter och IT-avdelningar arbetade med. IT-brottslighet, ID-kapningar och digitala intrångsförsök ökar markant och i dag utsätts vi alla för olika typer av IT-relaterad brottslighet eller försök därtill. Oftast utan att vi ens märker det. Våra enheter kan tas över för att till exempel utvinna information, för att genomföra IT-attacker på andra system eller för att ”gräva” kryptovaluta.

Vi jobbar målmedvetet för att skapa ett så gott skydd som möjligt för våra egna IT-system men då många medlemmar och förtroendevalda använder sig av egna, riksdagens, kommuners eller landstings IT-miljöer är det viktigt att alla också tar ett eget ansvar.

I den här skriften har vi satt samman goda råd för att hjälpa dig att förbättra din egen IT-säkerhet. Följ dem och stärk därigenom din egen IT-säkerhet. Var på din vakt!

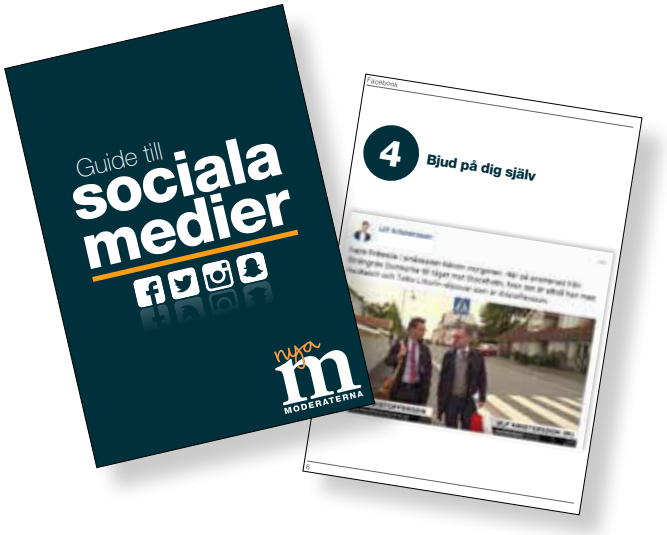
Anders Edholm
Vice partisekreterare

1 Visa omdöme i din digitala kommunikation

Allt du skriver kan hamna i orätta händer
Många av oss förutsätter att allt vi skriver i digitala kanaler såsom sms, messenger och e-mail är säkrat och att det bara är vi själva och den vi sänt meddelandet till som kan läsa det. Tyvärr är det inte så. Ditt lösenord kan komma på avvägar, din telefon kan bli stulen upplåst i ett obevakat ögonblick etc. Är du riksdagsledamot eller innehar annan senior position kan främmande makt försöka nå dina data med metoder som inte ens kräver ditt lösenord eller fysisk tillgång till din dator eller mobila enhet.

Tänk på vad du skriver. Var sparsam med personomdömen eller annat som kan upplevas som uppseendeväckande om det hamnar i orätta händer. Du ska förstås aldrig dela hemlig information genom öppna digitala kanaler. Tänk på att ett e-post-meddelande kan liknas vid ett vykort, öppet för alla att se.

Aktivitet på sociala medier är något vi uppmuntrar – testa dig fram och se vilka kanaler du är bekväm med och vilka typer av inlägg som fungerar. Vår uppgift är att alltid föra samtal med och hålla kontakt med väljarna och kontinuerligt föra ut vårt budskap. I foldern ”Sociala Medier” får du tips och råd kring din kommunikation i sociala medier.



2 Skydda dig mot intrång och ”phising”

Stulna lösenord, hackade konton och virus blir allt vanligare och riskerar att leda till att privat eller konfidentiell information från dina konton hamnar i orätta händer. Det finns dock effektiva sätt att skydda sig mot detta och det är viktigt att alla aktiva medlemmar vidtar säkerhetshöjande åtgärder.

Phising och spear-phising (nätfiske)
Många av oss har någon gång mottagit mail med uppmaning att ändra lösenord på vårt mailkonto eller annan tjänst. Klickar man på länken i mailet kommer man direkt till en sida för lösenordsbyte. Om du får ett sådant mail är risken väldigt stor att du är utsatt för ett phisingförsök. Phising, eller nätfiske, riktas mot en stor grupp människor medan spear-phising är ett liknande försök riktat mot en enskild person. I den amerikanska valrörelsen utsattes demokraternas kampanjchef för spear-phising. Kampanjchefen fick ett mail med en uppmaning att byta sitt Gmail-lösenord. Kampanjchefen var smart och skickade mailet vidare till sin IT-avdelning och frågade om han borde följa rådet. IT-avdelningen sa att det var OK så kampanjchefen klickade på länken. Klicket resulterade i att främmande makt kunde ladda ner kampanjchefens hela maildatabas inklusive känsliga mail mellan honom och presidentkandidaten.

Ett enkelt sätt att verifiera att du verkligen kommit till rätt webbsida när du klickat på en länk är att klicka på hänglåset högst upp på sidan i webbläsaren. Genom att klicka på hänglåset får du upp information om att ett certifikat är utfärdat till domänen du är på. Om du t.ex. går in på moderaterna.se så finns där ett certifikat som visar att det faktiskt är Moderaternas hemsida du är inne på. Att en webbsida utger sig för att vara någon annan än den verkligen är brukar kallas för ”spoofing”.

Vanliga virusskydd och malwareskydd fungerar inte alltid bra för att skydda mot phising och spearphising. Bästa skyddet är att vara på sin vakt och aldrig klicka på länkar i mail från främmande personer.

Ha alltid ett uppdaterat operativsystem
Ett enkelt sätt att öka säkerheten på dina mobila enheter och dina datorer är att alltid se till att ha den senaste versionen av operativsystemet. När du får meddelande att en ny version eller uppdatering av operativsystem finns tillgängligt, uppdatera omedelbart.

Var på din vakt!
Om du blir uppringd av någon som vill ha dina inloggningsuppgifter, eller ber dig logga in med Bank-ID, avsluta samtalet.

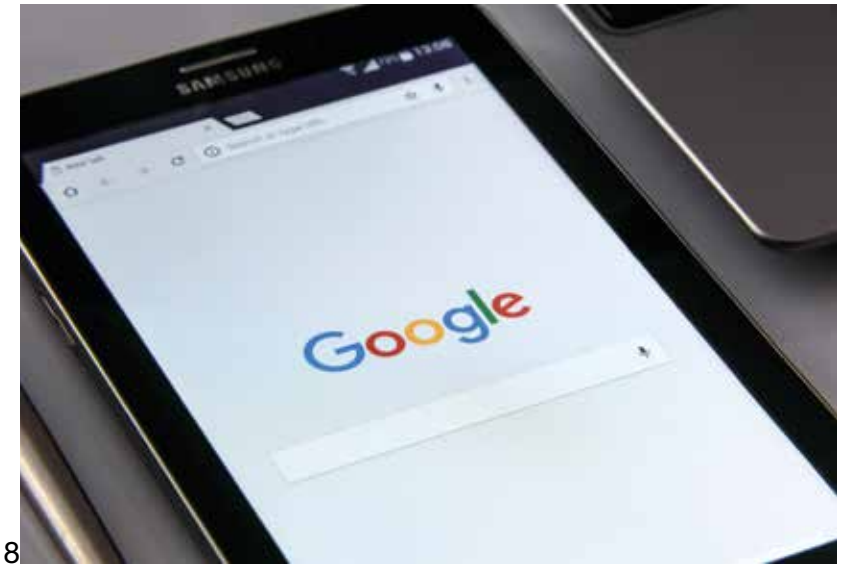
Virus och malware-skydd
Bäst skydd mot virus och malware får du genom att köpa ett virusskydd som automatiskt uppdateras regelbundet. Det finns många leverantörer att välja på t.ex Symantec/Norton, Fsecure och Panda. En leverantör vi avråder dig från att använda är ryska Kaspersky Labs, en leverantör som svartlistats i USA då man inte kan säkerställa att programvaran inte innehåller spionprogramvara.

Tvåfaktorsautentisering
Ett starkt lösenord är bra, två lösenord är bättre. Det är därför bra att använda sig av tvåfaktorsautentisering. Det är ett extra skydd till ditt konto som innebär att du förutom att skriva in ditt lösenord (som ej bör bestå av namn eller enskilda ord som finns i en ordlista), behöver verifiera att det är du som försöker logga in på ditt konto med en bekräftelse från något du äger.

Den vanligaste tvåfaktorsautentiseringen är att du får en kod skickad till din telefon som du sedan måste skriva in för att kunna logga in. Tvåfaktorsautentisering kan också ske med hjälp av en app som genererar engångskoder, t.ex. Google Authenticator.

Använd tvåfaktorsautentisering för ditt externa mailkonto, dina sociala-medier konton, molnlagringstjänster och betalningskonton. Mailkontot är allra viktigast eftersom du via mailen kan få åtkomst till andra konton och viktig information. Moderaternas e-mail skyddas genom att nya mobila enheter måste verifieras av IT-avdelningen innan enheten accepteras av systemet.

Tvåfaktorsautentisering är enkelt att komma igång med och det flesta hemsidor och plattformar erbjuder detta idag.



Så här gör du för att aktivera tvåfaktorsautentisering:

- Gör en lista på de plattformar du använder och sök efter hur två-faktorsautentisering fungerar på dem.
- Använder du ett Googlekonto kan du ladda ner Google Tvåfaktors-autentisering (Google Authenticator) som är en app som genererar engångskoder för alla dina Google-applikationer, men även till andra tjänster som Facebook och Dropbox.
- Om du har ett iCloud konto (Apple) så kan du aktivera tvåfaktors-autentisering för ditt konto och din iPhone, Mac eller iPad.
- Aktivera tvåfaktorsautentisering på ditt Facebook och Twitterkonto.

Du aktiverar tvåfaktorautentisering här:

Apple (iPhone, iPad, Mac):
https://appleid.apple.com

Google (Gmail, Android mm.):
https://www.google.com/landing/2step/

Facebook:
https://www.facebook.com/settings?tab=security

Twitter:
https://twitter.com/settings/account

3 Åtgärder för att minska risken för att bli utsatt för bedrägerier och ID-kapning

Varje år sker tiotusentals bedrägerier där personer tar över någon annans identitet och beställer varor online som offret får fakturan för. Aktivister kan också försöka ändra politiska motståndares folkbokföringsadresseer för att på så sätt tvinga bort dem från politiska uppdrag. Ett vanligt tillvägagångssätt är att offrets post vidaresänds så att mottagaren inte får brev om t.ex. begärd adressändring eftersom breven skickas till bedragaren.

Dessa åtgärder är viktiga att vidta för att minska risken för att bli utsatt för bedrägerier och ID-kapning.

- Logga in på Skatteverket och ställ in att Bank-ID ska krävas för att ändra din folkbokföringsadress.
- Gå till Adressändring.se och ställ in att Bank-ID ska krävas för att beställa vidaresändning av din post.
- Använd en gratis digital brevlåda för myndighetspost, så som Kivra.se eller Minmyndighetspost.se. Då skickas brev från anslutna myndigheter och företag dit istället för på papper.

4 Ta säkerhetskopior

Tänk igenom vad som skulle hända om du blev av med din telefon eller dator och behöver skaffa en ny. Har du en kopia på bilder och dokument?

Säkerhetskopiera alltid ditt innehåll, antingen på en extern hårddisk eller via en molntjänst.

5 Använd kryptering och bra lösenord på telefon och dator

Om du tappar bort eller blir av med din mobila enhet eller dator behöver informationen i enheten vara skyddad. Ställ in din dator så att lösenord krävs när du slår på datorn, men också när du ska aktivera datorn efter det att skärmsläckaren slagits på. Telefonen ska fråga om kod efter någon minuts inaktivitet. Datorns hårddisk ska vara krypterad.

Åtgärder:

- Använd minst sexsiffrig kod på din telefon och ställ in den så att du måste slå in koden varje gång telefonen varit inaktiv i någon minut. Ställ in så att telefonens minne raderas efter 10 felaktiga försök att låsa upp den

- Ställ in lösenord på datorn så att det alltid måste anges när man startar den och efter det att skärmsläckaren startat. Skärmsläckaren bör starta efter max fem minuters inaktivitet. Ha ett lösenord på minst åtta tecken, gärna fler, med både siffror och bokstäver, helst också stora och små bokstäver samt något special tecken. Använd inte ord som finns i ordlistan.

- Kryptera datorns hårddisk. Både Mac och Windows har inbyggda krypteringsfunktioner som du kan slå på.

6 Ytterligare verktyg för att höja din säkerhet

Virtuellt privat nätverk – VPN (tunnel)
Om du använder trådlösa nätverk på offentliga platser (café, tåg osv.) bör du använda ett VPN (t.ex. Freedome från Fsecure eller ProtonVPN). VPN är en krypterad nätverksuppkoppling som gör att andra på samma plats inte kan avlyssna din internetuppkoppling och komma åt lösenord eller annan känslig information.

Det finns automatiska verktyg som letar efter osäkra uppkopplingar och det förekommer också att personer ”erbjuder” gratis internet och döper nätet till ”Free wifi” eller motsvarande, och avlyssnar trafiken. Vid senaste Folk & Försvar-konferensen i Sälen satte aktivister upp ett öppet nätverk som många deltagare kopplade upp sig mot – helt okrypterat. Koppla aldrig upp dig mot ett sådant nätverk om du inte har VPN.

Lösenordshanterare
En lösenordshanterare sparar dina lösenord så att du istället kommer åt dem med ett enda lösenord. Eftersom du inte behöver komma ihåg lösenorden själv kan du använda lösenord som är olika för varje tjänst, vilket ökar säkerheten. Det vill säga, du bör ha olika lösenord för iCloud, gmail, inloggningen på din dator osv.

En vanlig säkerhetsbrist är att man använt samma lösenord på flera platser och den plats med lägst säkerhet fått ett intrång, som sedan gör att ens andra konton också går att komma åt.

Lösenordshanterare finns inbyggt i din iPhone/iPad men det finns även tillförlitliga tredjepartsprogramvaror som t.ex. 1Password och Dashlane.

Tejpa över kameran (och kanske mikrofonen) på din dator
Om du råkar ut för att spyware installeras på din dator finns det risk för att förövaren kan ta över kameran och mikrofonen utan att du märker det. Ett enkelt skydd är att tejpa över kameran (och även mikrofonerna om man vill känna sig riktigt säker).

7 Hot och trakasserier på nätet

Sociala medier är bra och viktiga verktyg i det politiska arbetet, men det har sina baksidor. Det hårda samtalsklimatet och möjligheten till anonymitet bidrar till att det förekommer hot, hat och trakasserier i digitala kanaler.

Brottsförebyggande Rådet kartlägger hot och trakasserier mot förtroendevalda i sin återkommande rapport, Politikernas trygghetsundersökning (PTU). En av fyra politiker utsattes för trakasserier år 2016, visar rapporten. Det vanligaste var att hoten och trakasserierna skedde genom sociala medier, men även via telefon och i verkligheten.

I skriften att förhindra och förebygga incidenter mot förtroendevalda, har Brottsförebyggande rådet pekat ut några riskgrupper, det vill säga personer som löper en högre risk att utsättas för incidenter. Följande grupper pekas ut som riskgrupper av BRÅ.

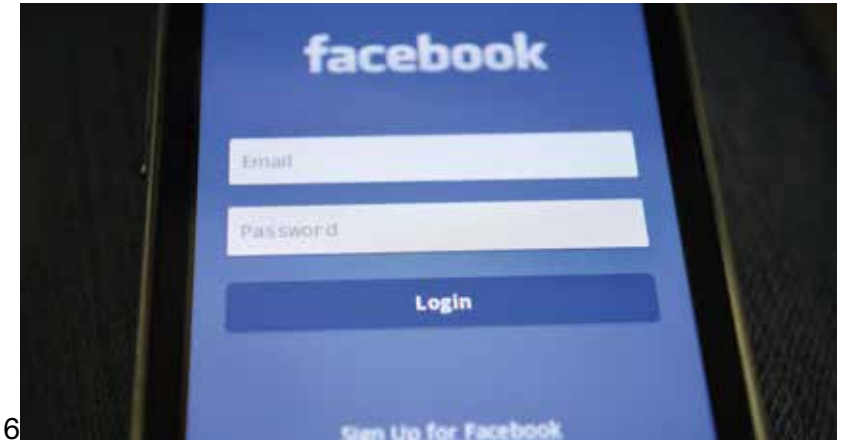
- yngre förtroendevalda
- heltidspolitiker
- nämndordföranden
- ledamöter i kommun- och landstingsstyrelser
- förtroendevalda som syns mycket och är aktiva i sociala medier

Nedan finner du förslag på ett antal åtgärder som är viktiga för att förebygga att du blir utsatt för hot och trakasserier i sociala medier, samt hur du ska agera om du blir utsatt.

Förebyggande åtgärder
Säkerhetspolisen har i sin handbok, personlig säkerhet, tagit fram ett antal råd för hur politiskt aktiva ska agera i säkerhetsfrågor.

En viktig utgångspunkt i det arbetet är att vara personlig men inte privat i sin kommunikation, att vara allt för utelämnande om sina personliga förhållanden kan skapa en säkerhetsrisk.

Det kan även vara bra att inte i förväg berätta var du ska befinna dig. Det bör även beaktas att användning av incheckningsfunktioner på sociala medier utgör en säkerhetsrisk och bör användas med försiktighet. I många fall kan det vara bättre att berätta om saker du har gjort och inte om saker du ska göra, för att undvika kartläggning eller att personer söker upp dig.



Undvik även att exponera eller ge inblick i dina dagliga vanor, då detta kan underlätta kartläggning av dina vanor och rörelsemönster. Försiktighet bör iakttas vad gäller i vilka butiker du handlar, var du tränar och övriga platser du ofta besöker.

Var även tydlig gentemot vänner och familj vad som gäller för din medverkan i sociala medier. Om du bedömer att det föreligger en hotbild mot dig bör du uppmana din familj att undvika angivelse av geografisk plats om du medverkar på en bild.

Det är viktigt att du aldrig kommenterar din egen säkerhet eller skyddsåtgärder som rör dig eller dina närstående. Dessa uppgifter kan få snabb spridning på sociala medier och kan bidra till att en eventuell gärningsperson kan kartlägga dig. Du bör inte heller i affekt kommentera om du blivit utsatt för hot eller trakasserier.

Även om du själv inte blir utsatt för hot eller trakasserier, bör du även avhålla dig från att kommentera skyddsåtgärder för andra i partiet. Av samma bevekelsegrunder som gör att du inte ska kommentera dina egna skyddsåtgärder, ska du inte kommentera andras.

Du kan även ta bort dina privata uppgifter från söktjänster som Eniro och Hitta.se. Det kan ta lång tid och är inte alltid enkla processer, men är ett viktigt verktyg i det säkerhetshöjande arbetet.

Kontroverser och ryktesspridning
Algoritmerna i sociala medier premierar material som fått mycket engagemang och reaktioner. Därför får det som publiceras ofta snabb spridning. Det gäller även falsk, vilseledande information eller ren desinformation.

Det är viktigt att vara vaksam på rykten, falsk information och kontroverser i sociala medier. Som politiska företrädare har vi ett ansvar i att bemöta eller dementera uppgifter som inte stämmer. Om du upptäcker något i sociala medier som du bedömer vara antingen falsk information, accelererande ryktesspridning eller desinformation så bör du ta en skärmavbild och skicka den till din partiombudsman.

Stalkning
Med stalkning avses upprepad förföljelse eller trakasserier från samma person. Politiskt aktiva löper större risk att bli utsatta för stalkning än andra. Försök att undvika all kontakt med personen som utsätter dig för stalkning och besvara inte meddelanden i sociala medier eller e-post från personen.

Spara alla meddelanden du fått från personen. Dessa utgör viktigt underlag när du ska göra en polisanmälan. Om det finns en risk för fysisk konfrontation med stalkern bör du försöka att förändra dina rörelsemönster, så att du inte befinner dig i samma butik varje dag vid en viss tidpunkt och ta inte samma väg hem från jobbet.

Upplever du att trakasserierna inte är övergående bör du i samband med din polisanmälan begära att polisen beslutar om kontaktförbud, vilket innebär att stalkern förbjuds att kontakta dig.

Hantera hot och trakasserier
Det är inte acceptabelt att bli utsatt för hot eller trakasserier på grund av sitt politiska uppdrag. Det är i förlängningen ett hot mot demokratin att allt fler politiskt aktiva lämnar sina uppdrag på grund av hot och trakasserier. Det är därför viktigt att du känner till hur du ska agera om du blir utsatt. Här är ett antal åtgärder som är viktiga att vidta:

- Ta skärmdumpar
- Polisanmäl alltid
- Meddela din partiombudsman
- Är du förtroendevald inom kommun eller landsting ska du ta kontakt med församlingens säkerhetsansvarige.
- Riksdagsledamöter tar kontakt med Säkerhetspolisen enligt deras anvisningar.

För mer information, tips och idéer kring personlig säkerhet se denna publikation från Säkerhetspolisen:

http://www.sakerhetspolisen.se/publikationer/rapporter-amnesvis/sakerhetsskydd/personlig-säkerhet.html


nya
MODERATERNA