Cyber guiden

Digital säkerhet för alla

Panu Moilanen och Irina Lönnqvist

Varför behöver du denna guide?

Vi lever i en värld som i allt större utsträckning är digital och allt mer beroende av bland annat informationssystem, digitala tjänster och dataförbindelser. Digitaliseringen är först och främst till nytta för oss: den gör livet säkrare, effektivare och roligare. Digitaliteten omfattar emellertid också säkerhetsrisker.

Digitaliseringen förändrar säkerheten på två sätt. Teknisk påverkan på eller via den digitala världen brukar vanligen kallas cyberhot, cybersäkerhet och till och med cyberkrigföring.

När till exempel vårt tänkande påverkas genom påverkan på eller via information i den digitala världen talar vi om informationshot, informationssäkerhet och till och med om informationskrigföring.

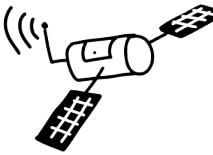
Via den digitala världen kan även data påverkas – till exempel stjälas eller manipuleras. Vårt samhälle är allt mer beroende av olika stora informationslager och det är viktigt att säkerställa lagrens konfidentialitet, tillgänglighet och integritet, dvs. oföränderlighet. Ett exempel på ett stort informationslager är Kanta-tjänsten som innehåller hälsouppgifter. Vi har alla dessutom personliga viktiga data som måste skyddas.

Förändringarna i Finlands och Europas säkerhetssituation påverkar också den digitala säkerheten. Den instabila säkerhetsmiljön återspeglas också i den digitala världen i form av konflikter och operationer. En del av dessa kan vara skadliga och till och med farliga för oss.

I den digitala världen stämmer uttrycket att en kedja är precis så stark som dess svagaste länk. Vi är alla länkar i olika kedjor av digital säkerhet. Dessa kedjor säkerställer inte bara vår egen utan också vår familjs, våra närmiljöers och hela Finlands digitala säkerhet. Därför är det viktigt att vi alla känner till grunderna i digital säkerhet.

Den digitala världen

Den digitala världen låter kanske som något som bara experter behöver förstå sig på. Så är det däremot inte, utan digitaliseringen berör oss alla. I nästan alla ärenden vi sköter i vår vardag används numera informationssystem, informationsnät och program – det vill säga den digitala världen. Digitaliseringen utvecklas också hela tiden.



Den digitala världen kan anses bestå av en teknisk cybermiljö och olika digitala informationsmiljöer. I cybervärlden består allt av bitar, dvs. informationsbärande enheter. Det är ungefär detsamma som att allt i den fysiska världen består av atomer. Bitvärlden och atomvärlden är allt oftare sammanflätade. Tv:n är ett fysiskt föremål som ändå behöver bitar för att fungera. På samma sätt behövs samspel mellan atomer och bitar till exempel inom handeln, hälsovården och trafiken.

Informationsmiljön är en miljö som består av användare, informationsnät, tjänster och information, där information samlas in, behandlas, lagras, förmedlas, skyddas och används. Det finns information av många olika slag, till exempel data som överförs mellan olika informationssystem eller kommunikation och växelverkan människor emellan.

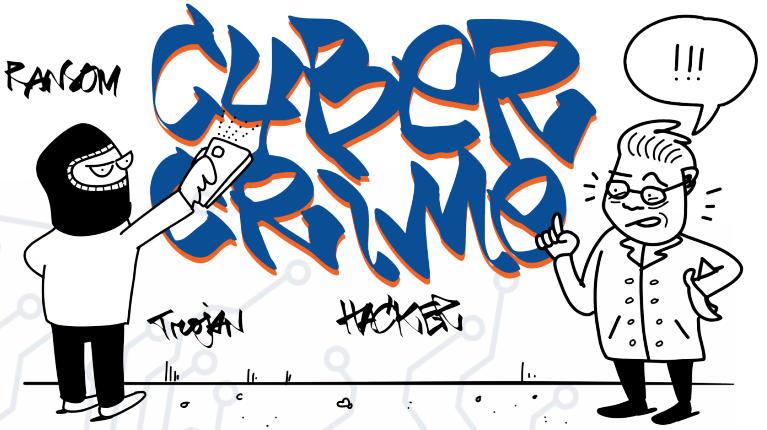
Alla har säkert hört berättas om hur vanliga medborgares liv har påverkats av funktionsstörningar i olika informationssystem. Det har inte gått att betala inköp med kort i närbutikens kassa eller att

logga in i nätbanken eller stadstrafiken har stockat sig då systemet som styr trafikljusen har råkat i oordning. I alla dessa situationer är det fråga om att störningar i den digitala världen också har påverkat verkligheten.

Cyberordlista

Den digitala världen är en miljö som är avsedd för behandling av digital information och som består av datorer och andra enheter, datanät, tjänster och användare som är kopplade till varandra. Den kan anses bestå av en teknisk cybermiljö och olika digitala informationsmiljöer.

Digitala hot eller cyberhot betyder risk för en handling eller en händelse som äventyrar den digitala världens rätta och felfria funktion om hotet förverkligas. Hotet kan till exempel vara ett skadligt program, ett överbelastningsangrepp eller dataintrång. Ofta störs den digitala världen också av en helt slumpmässig händelse, till exempel felaktig användning, en störning i datakommunikationen eller ett elavbrott.



Digital säkerhet innebär att olika hot riktade mot den digitala världen är under kontroll och att den digitala världen fungerar rätt och felfritt. Digital säkerhet kan indelas i cyber- och informationssäkerhet. En del av den digitala säkerheten är att alla medborgare handlar rätt och ansvarsfullt i den digitala världen.

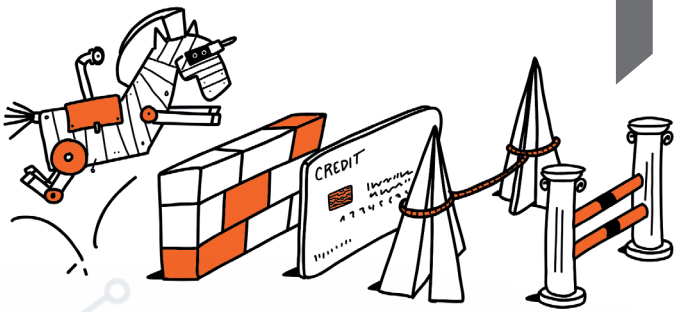
Skadliga program är program vars syfte är att orsaka olägenheter eller skador på datorer, andra smarta enheter eller via dem till exempel för användarna eller andra objekt. Skadliga program är bl.a. virus, utpressningsprogram, spionprogram och bakdörrar. Skadliga program borde kunna hindras från att komma in i enheterna.

Hybridpåverkan är vanligen fientlig verksamhet som en statlig aktör genomför direkt eller via andra aktörer. Aktören strävar till exempel efter att genom politiska, militära eller ekonomiska åtgärder eller cyber- och informationspåverkan påverka samhället i syfte att få det att vackla. Ofta används många metoder samtidigt för att skapa bl.a. rädsla, osäkerhet och polarisering. Den digitala världen är en av de främsta miljöerna för hybridpåverkan.

Informationspåverkan är påverkan på den tillgängliga informationens innehåll och spridning samt därigenom på slutresultatet av en händelseserie i olika skeden. Målet kan till exempel vara att påverka medborgarnas åsikter. Informationspåverkan kan också vara fientlig. Detta kallas svart informationspåverkan. När den är förknippad med en pågående konflikt eller genomförs av en statlig aktör kan man också tala om informationskrigföring.

Utpressningsprogram är skadliga program som vanligtvis krypterar innehållet på en dator eller någon annan smart enhet. Därefter pressas ägaren till enheten på lösen (vanligtvis pengar i kryptovaluta). I gengäld utlovas dekrypteringsanvisningar. Lösen bör inte betalas. Det går att skydda sig mot utpressningsprogram med hjälp av säkerhetsprogram och säkerhetskopiering.

Kritisk infrastruktur avser alla tjänster, system och strukturer som utgör samhällets vitala funktioner. Exempel på kritisk infrastruktur är bland annat energidistribution, datakommunikationsnät, hälso- och sjukvården och dess informationssystem samt betalningssystem. Den kritiska infrastrukturen och den digitala världen är sammanflätade. Den kritiska infrastrukturen är det mest sannolika objektet för fientlig cyberpåverkan.



Cyberförsvar är ett delområde inom cybersäkerheten som gäller försvaret. Hit hör underrättelseverksamhet i och i anknytning till cybermiljön, skydd av cybermiljöer som är viktiga för landets försvar och påverkan på vissa cybermiljöer. I Finland ansvarar Försvarsmakten för cyberförsvaret.

Overbelastningsangrepp (DoS) är nätangrepp som försöker förhindra normal användning av en viss webbtjänst. Oftast genomförs angreppet genom att rikta en så stor mängd tjänsteanrop och nättrafik till tjänsten att tjänsten inte längre kan utföra sina uppgifter. Överbelastningsangrepp är de vanligaste tekniska cyberangreppen. Samtidigt är de också angrepp på informationsrummet, eftersom de ofta förhindrar tillgången till information till exempel på mediernas eller myndigheternas webbplatser.

Phishing, dvs. nätfiske, är åtgärder i syfte att få tillgång till konfidentiell information, till exempel person- eller kontouppgifter. Avsändaren ger sig ut för att vara en aktör som har rätt att få informationen. Uppgifterna kan sedan användas till exempel för att få ekonomisk nytta. Man ska vara mycket försiktig med att lämna ut personliga uppgifter på nätet.

Molntjänst är en tjänst som tillhandahåller lagringsutrymme på nätet. Uppgifter som lagras i en molntjänst lagras i stora serverhallar och används via nätet. Molntjänster kan användas till exempel för säkerhetskopiering av uppgifter. Det är ändå bäst att inte lagra särskilt personliga uppgifter i molntjänsterna. Det är inte heller alltid tillåtet att lagra konfidentiella eller hemliga uppgifter i molntjänsterna, till exempel arbetsrelaterade handlingar.

Uppdatering (programuppdatering) innebär att programvaran ändras så att den tidigare versionen ersätts med en ny programversion, t.ex. för att korrigera fel och säkerhetsluckor eller lägga till nya egenskaper. Programuppdateringar behövs för allt fler anordningar – datorer, mobila enheter, nätverksutrustning och till exempel hushållsapparater. Säkerställ att du känner till vilka alla anordningar som har program som ska uppdateras.

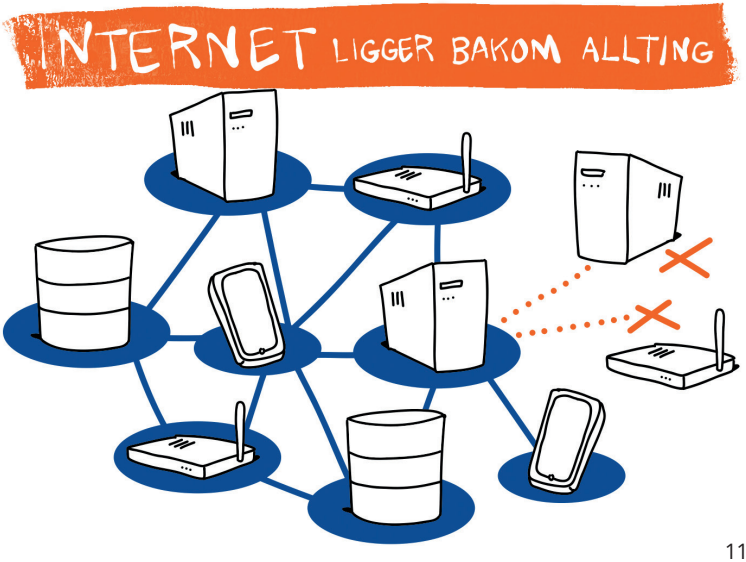
Djupfejk eller deep fake är en bild-, ljud- eller videofil som skapats med artificiell intelligens och som framstår som äkta men inte är det. Det går att skapa filer där till exempel republikens president säger någonting som han aldrig har sagt eller aldrig skulle säga. Det är också möjligt att byta ut människors ansikten i befintliga videor eller förfalska en persons röst digitalt.

Artificiell intelligens är teknologi som på sätt och vis kan utföra intelligenta funktioner. Exempel på dessa funktioner är bl.a. röstidentifiering, översättning av språk och produktion av olika slags innehåll. Det är stor nytta med artificiell intelligens, men den kan också användas i bedrägerier och fientlig informationspåverkan.

Informationssäkerhet avser alla sådana arrangemang som syftar till att säkerställa informationens användbarhet, integritet och konfidentialitet. Till informationssäkerheten hör bland annat att trygga information, utrustning, programvara, datakommunikation och verksamheten. På individnivå innebär informationssäkerhet att skydda viktiga uppgifter och enheter. Var och en ansvarar för sin egen informationssäkerhet.

Säkerhetskopiering innebär att viktig information kopieras och lagras även någon annanstans än på den ursprungliga platsen. Om den ursprungliga informationen försvinner eller förstörs kan informationen återställas från säkerhetskopiorna. Det är klokt att säkerhetskopiera innehållet till exempel i datorer och mobila enheter. Det är ofta bra att lagra säkerhetskopior både på en extern minnesenhet och i en molntjänst.

Nätverksenhet är en enhet via vilken andra enheter ansluts till internet. Enheten kan till exempel vara en router som kopplas till fastighetsnätet eller en mobil router som kopplas till mobilnätet. Det är mycket viktigt att säkerställa nätverksenheternas säkerhet. När du börjar använda nätverksenheten ska du byta det förvalda lösenordet. Kom också ihåg att uppdatera nätverksenheten regelbundet. Kontrollera om du behöver fjärradministration för nätverksenheten. Stäng av den om den inte behövs.



Inloggning kan jämföras med en nyckel

Vi loggar alla in i olika enheter och tjänster dagligen. Inloggningen är som en nyckel: den ger åtkomst till exempel till våra personliga uppgifter, pengar, minnen och mycket annat. Därför är det viktigt att ta lika bra hand om inloggningsuppgifterna som om hemnyckeln och säkerställa att inloggningsmetoderna alltid är tillräckligt starka och säkra.

Det vanligaste inloggningssättet är användarnamn och lösenord. Det är viktigt att lösenorden är tillräckligt starka – sådana som inte kan knäckas genom att gissa eller räkna ut dem. Ju längre lösenordet är desto bättre. Det går att komma ihåg även ett längre lösenord när det är en lösenfras – till exempel NaturenÄrVackerIdag2024!!.

Att använda dialektord eller annars ovanligare ord och lägga till specialtecken och siffror gör lösenordet ännu starkare.

I många tjänster kan multifaktorsautentisering också användas (MFA). Det betyder att det inte räcker med användarnamn och lösenord för att logga in,

utan inloggningen måste ännu verifieras till exempel med hjälp av en mobiltelefon och en engångskod. Om multifaktorsautentisering är tillgänglig i tjänsten är det klokt att alltid använda den.

Ett vanligt alternativ är också biometrisk inloggning, dvs. inloggningen sker till exempel med fingeravtryck eller ansiktsbild. Detta är i de flesta fall en bra kompromiss mellan säkerhet och användarvänlighet. Biometrisk identifiering är inte oproblematisk: ägarskapet när det gäller biometriska uppgifter och relaterade frågor om integritetsskyddet är fortfarande aktuella i stor omfattning.

Information är ett verktyg för maktutövning

Det sägs att kunskap är makt. Därför förekommer hela tiden försök att påverka kunskapen – dvs. informationen. Exempel på denna påverkan i vår vardag är reklam eller upplysningskampanjer där avsikten är att få oss att äta hälsosammare eller motionera mer. Det är godtagbar påverkan, dvs. vit informationspåverkan. Om målen med påverkan däremot är fientliga och illasinnade är det fråga om svart informationspåverkan eller informationskrigföring.

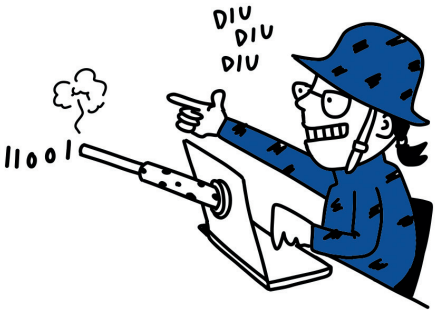
Svart informationspåverkan är fientlig påverkan på medborgarna, beslutsfattarna och funktionsförmågan genom att manipulera den tillgängliga informationen. Målet är att skada dem som är föremål för påverkan och de samfund de bildar.

Sociala medier och digitaliseringen har gjort informationen till ett ännu viktigare verktyg för maktutövning än tidigare. Mängden information är allt större och informationen sprids snabbare än tidigare. Därför har informationsmiljöerna blivit en väsentlig del av konflikter och krigföring.

Informationskrigföringen är alltid förknippad med en pågående konflikt. Det innebär fientlig påverkan på det utvalda objektets beslutsfattande, funktionsförmåga och åsikter via informationsmiljön samt skydd mot sådana försök att påverka.

De främsta fientliga statliga aktörerna i informationsrummet är ur finländsk synvinkel Ryssland och Kina, men även många andra stater gör sig skyldiga till informationskrigföring.

I den ryska krigföringen spelar informationskrigföringen en mycket viktig roll: enligt det ryska sättet att tänka förs krig alltid också på informationsnivån. Föremål för det ryska informationskriget är bland annat Europeiska unionen och Finland, och målet är t.ex. att ifrågasätta demokratiska värderingar, att skapa söndring i och upplösa unionen och samhällena och att skapa instabilitet i EU-länderna.



Under de senaste åren har utvecklingen av artificiell intelligens också förändrat den fientliga informationspåverkan avsevärt. Med hjälp av artificiell intelligens går det att skapa mycket trovärdigt men helt artificiellt medieinnehåll som kallas djupfejk (deep fake). AI-botar kan delta i diskussioner i sociala medier och sprida desinformation, dvs. osann information.

Det effektivaste sättet att skydda sig mot fientlig informationspåverkan är att använda sunt förnuft. Tänk alltid noggrant efter vad informationen betyder och om den kan vara sann. Vem har publicerat meddelandet och vad kan motivet eller målet vara? Kan du kontrollera via andra källor om informationen är sann? Och framför allt ska du tänka efter först: innan du gillar, delar, blir arg eller gör något annat. Håll huvudet kallt och tankarna klara! På så sätt utvecklar du också din medie- och multilitteracitet, som är viktiga medborgarfärdigheter i den digitala miljön!

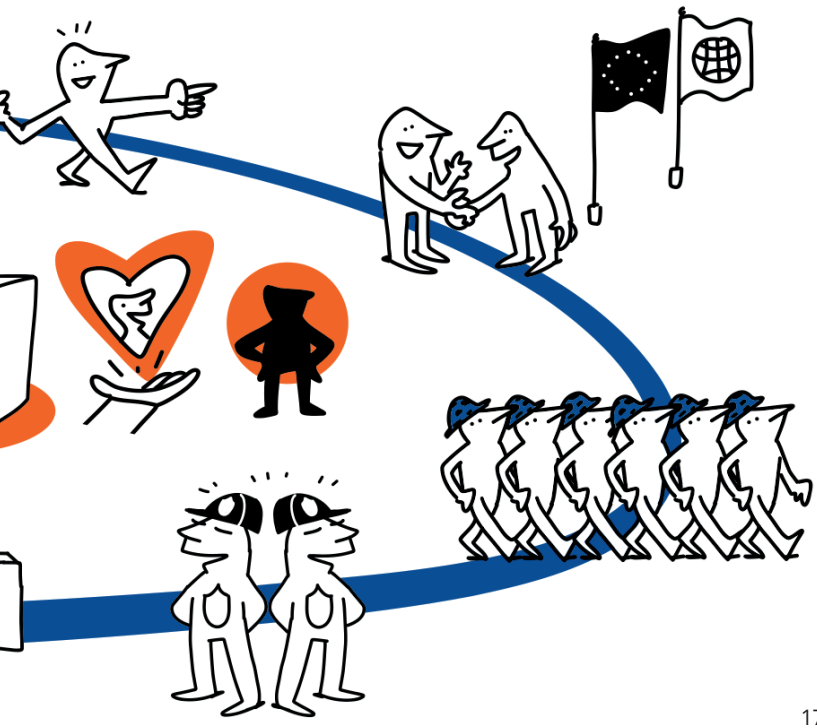
Det är klokt att vara förberedd

Även om mycket har förändrats i och med digitaliseringen är beredskap ändå fortfarande det viktigaste för att säkerställa att olika störningssituationer kan klaras av.

Störningar i vardagen är förtretliga och i värsta fall kan de också orsaka betydande skada och till och med fara. Framför allt innebär de dock en psykisk belastning: en störning i de normala funktionerna och rutinerna kan rubba trygghetskänslan och skapa osäkerhet. Detta är normalt och det är bra att redan på förhand fundera på hur vi klarar oss om de grundläggande funktionerna i vårt samhälle

i något skede inte fungerar normalt till exempel på grund av problem i den digitala världen eller av någon annan orsak.

Det finns mycket kunskap till hands som hjälper dig att fundera på den egna överlevnadsstrategin. Omfattande anvisningar om hur du förbereder dig inför kris- och störningssituationer hittar du enklast på webbplatsen suomi.fi. Det är bra att göra sig förtrogen med anvisningarna genast: de tar upp olika störningssituationer allt från översvämningar till strålningsolyckor.



Med tanke på den digitala säkerheten är det bra att förbereda sig åtminstone på följande sätt:

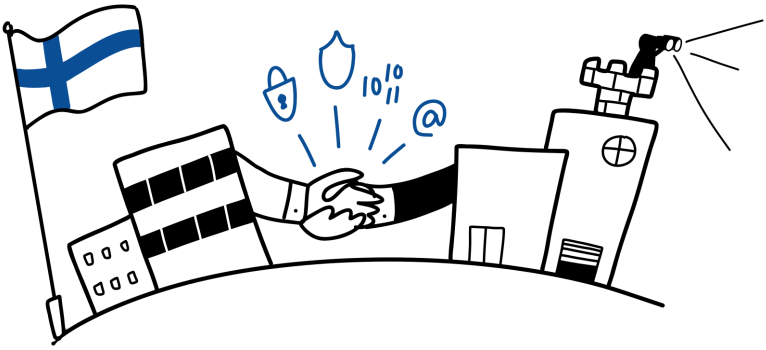
1. **Läs** de tio budorden för digital säkerhet på baksidan av denna guide och följ dem.
2. **Säkerställ** att du har tillgång till åtminstone två metoder för stark autentisering när du använder digitala tjänster. För stark autentisering kan man i Finland använda till exempel bankkoder, mobilcertifikat och elektroniskt identitetskort. Internationellt används till exempel den europeiska digitala identitetsplånboken.
3. **Förbered** dig på att betalningssystemen och penningrörelsen inte alltid fungerar. Ha kontanter åtminstone där hemma och överväg också att sprida betalningsrisken till exempel genom att ha konton i olika banker eller använda olika aktörers betalkort.
4. **Fundera** på hur du får information och håller kontakt med dina närstående vid störningar i datatrafiken eller eldistributionen. Ha en batteridriven radio och reservströmkällor till hands där hemma. Se till att reservströmkällorna är laddade.
5. **Följ** myndigheternas och andra tillförlitliga aktörers anvisningar om digital säkerhet. Ta för vana att t.ex. läsa Cybersäkerhetscentrets meddelande om cybervädret varje månad.
6. **Det viktigaste är att hålla sig lugn** och komma ihåg att vi klarar det här! Om inte ensamma så åtminstone tillsammans!

Var en länk i en stark kedja!

Som vi konstaterade i början berör den digitala säkerheten oss alla och färdigheterna i digital säkerhet är numera medborgarfärdigheter.

I den digitala världen måste alla känna till de grundläggande reglerna och vara försiktiga och uppmärksamma – precis som i trafiken. I trafiken kan redan en enskild tönt orsaka allvarlig skada. Situationen är densamma i den digitala världen. Enklast hittar du omfattande anvisningar om beredskap för kris- och störningssituationer på adressen **www.suomi.fi/guider/beredskap**. Därför är det viktigt att vi säkerställer både vårt eget och våra närståendes kunnande. På så sätt försäkrar vi oss om att vi inte är de svagaste länkarna i den digitala säkerheten. Samtidigt stärker vi den digitala säkerheten i hela Finland.

På baksidan av denna guide hittar du de tio budorden för digital säkerhet som utarbetats för medborgarna. Med hjälp av dessa förbättrar du din egen och även andras digitala säkerhet. När du följer dessa bud och andra anvisningar i guiden är du en länk i den starka kedjan av digital säkerhet!l



Vill du veta mer?

Blev du intresserad av digital säkerhet och vill veta och lära dig mer om den? Både Försvarsutbildningsföreningen MPK och Jyväskylä universitet som publicerat denna guide ordnar kurser i digital säkerhet som är tillgängliga för alla.

Du får information om tillgängliga kurser på adressen **mpk.fi/kyber** och **r.jyu.fi/digiturva**

Välkommen!

TEXT

Panu Moilanen
Irina Lönnqvist

ILLUSTRATION

Linda Saukko-Rauta
Redanredan Oy, 2017–2022

LAYOUT

Ossi Hietala, Suvi Karjalainen

UTGIVARE

Jyväskylä universitet
Försvarsutbildning MPK

TRYCKÅR

2025

TRYCKERI

PunaMusta Oy

ISBN

ISBN 978-952-86-1119-6 (tryckt)
ISBN 978-952-86-1120-2 (pdf)

MPK
MAANPUOLUSTUSKOULUTUS
FÖRSVARSUTBILDNING

JYU. Since 1863.

ICT
SUOMI

De tio budorden för digital säkerhet till medborgaren

1. **Var sunt skeptisk** och fråga VARFÖR tillräckligt ofta.
2. **Tänk efter vad du publicerar på nätet:** det är inte nödvändigt att berätta allt och det som publicerats på nätet fås inte bort efteråt.
3. **Klicka inte på länkar** och öppna inte bilagor om du är osäker på om de är säkra. Gå aldrig till inloggningssidan för en tjänst t.ex. via en länk i ett sms eller ett e-postmeddelande.
4. **Kom ihåg att uppdatera alla dina apparater** och säkerställa att de är datasäkra – även t.ex. hushållsapparater. Be om råd om du inte vet vad du ska göra! Informationssäkerheten får inte vara föremål för sparåtgärder!
5. **Var särskilt försiktig när det är fråga om pengar.** Sörj för att dina bankkoder är i säkerhet och använd till exempel mobilcertifikatet för allmän identifiering.
6. **Kom ihåg att offentliga och öppna trådlösa nätverk** inte är säkra. Använd inte offentliga enheter för sådant som kräver inloggning. Låna inte dina enheter till personer du inte känner.
7. **Kom ihåg att ta säkerhetskopior**. Lagra säkerhetskopior både på externa minnesenheter och i molntjänster. Använd automatisk säkerhetskopiering om möjligt.
8. **Använd tillförlitliga och säkra inloggningssätt.** Lösenordet ska vara tillräckligt långt. Använd multifaktorsautentisering alltid när det är möjligt.
9. **Fundera redan på förhand** på hur du skulle klara dig i vardagen även utan den digitala världen och dess tjänster. Förbered dig också konkret!
10. **Var försiktig, men var inte rädd** – den digitala världen är till klart större nytta än skada. Ge också hjälp och stöd till andra om du kan och om det finns ett behov.