PHATHACKZ

Digital integritet

Ett häfte med enkla tips för dig som vill skydda ditt ***digitala*** *liv*

0
0
0
1
X

“One man's trash, another man's treasure”

Information sprids snabbt och fritt på internet. Du kanske lägger upp ett foto, delar vad du har gjort, vilka du har varit med, och taggar platsen med en kommentar om hur fantastisk dagen varit. Denna information når ditt nätverk av vänner, familj och bekanta på sociala medier. År senare kan du bläddra tillbaka och återupptäcka minnen – platser du besökt och vad du gjort. Du kanske tror att denna information endast når de människor du bryr dig om, som vänner, familj och kollegor. Men oftast så finns informationen tillgänglig utanför vår lilla bubbla.

Vem äger egentligen informationen? Och vem kan se vad jag lägger ut?
När du använder olika plattformar är det plattformen som styr hur din information hanteras. Har du läst villkoren innan du skapade ditt konto? Många gånger används din data för att säljas vidare till marknadsföringsföretag, eller för att anpassa reklam som påverkar ditt liv. Din information kan även hamna i fel händer – hackare, inbrottstjuvar och andra kriminella kan använda den för att kartlägga dig, skada dig eller kapa din identitet och begå bedrägerier i ditt namn. Det är viktigt att vara medveten om hur dina uppgifter används och skyddas.

Din digitala information samlas in dagligen av olika appar för att bättre förstå dig som användare. Denna data kan kartlägga ditt liv i detalj – när ditt alarm ringer, vad du gör direkt på morgonen, vilka platser du besöker, eller vilken buss du tar till jobbet eller skolan. Kanske till och med om kaffet smakade bra på Pressbyrån klockan 08:13 vid centralstationen.

Utan att låta för dystopiskt, är syftet med detta häfte att öka din medvetenhet om hur du rör dig online och ge dig enkla åtgärder för att skydda ditt digitala liv. Eftersom den digitala världen förändras snabbt, kan tips och råd variera, men det är alltid du som ansvarar för din egen integritet och hur du använder olika appar och tjänster. Ibland kan vi inte göra så mycket åt saken. Vi behöver helt enkelt kunna kommunicera med andra, delta i forum och hålla kontakt med människor. Livet har blivit enklare på den fronten och det finns givetvis många fördelar också.

Detta häfte uppdateras regelbundet för att ge dig den senaste och mest relevanta informationen om hur du skyddar din digitala integritet.
Här hittar du enkla metoder för att förbättra din säkerhet utan att behöva använda krånglig teknik eller dyra tjänster. Andra delar av häftet går igenom mer tekniska lösningar som kan göra ditt digitala liv både enklare och säkrare. Kom ihåg att det är du som har kontrollen över hur din information hanteras. Även om viss information kanske inte känns riskfylld för dig, kan det vara just den informationen som en angripare letar efter. Det är svårt att helt undvika digitala fotspår, men med hjälp av denna handbok kan du stärka skyddet kring din digitala identitet.

PHATHACKZ

_01____Öka din medvetenhet om cybersäkerhet

Att bli mer medveten om cybersäkerhet är en stark grund för att skydda sig online.
Det finns mängder av program och lösningar som kan hjälpa dig men det gäller att börja med rätt tankesätt för att få ökad förståelse.

1. **Publika nätverk**: När vi använder publika nätverk är det viktigt att komma ihåg att vi inte äger eller har kontroll över dem. Kontrollera alltid nätverkets namn noggrant innan du ansluter och undvik automatisk anslutning. Publika nätverk kan sättas upp av okända personer som ger nätverket namn som till exempel "Espresso House WiFi", i ett försök att genomföra en attack där de låtsas vara ett legitimt nätverk och kan övervaka din kommunikation. Om du måste använda publika nätverk, rekommenderas att alltid använda en VPN-tjänst. Jag rekommenderar Mullvad VPN, som också hyllas av många säkerhetsexperter och är ett starkt alternativ tack vare deras höga standard för datalagring, integritet och stabil anslutning.

2. **Lämna aldrig ifrån dig din mobil/dator/dokument obevakat:** Tyvärr är detta något som sker alltför ofta. Det är vanligt att se människor lämna sin dator olåst, mobilen obevakad på bordet, eller viktiga dokument synliga på publika platser som caféer, tåg, co-working spaces och bibliotek. Ett säkerhetstänk du bör ta till dig är att alltid ha koll på dina egna prylar och vara medveten om risken att de kan hamna på fel ställen.

3. **Tänk efter en extra gång innan du lägger upp något på sociala medier:** När du delar information om dig själv på sociala medier förlorar du ofta kontrollen över hur den hanteras och vem som ser den. Föreställ dig en inbrottstjuv som ser dina bilder på ditt nyrenoverade hem. Du visar inte bara hur fint det blivit, utan även vilka värdefulla föremål du har och vilka områden i ditt hem som kanske saknar övervakning. På så sätt hjälper du omedvetet till att kartlägga ditt eget hem och dina dagliga rutiner. Om du dessutom lägger ut att du ska åka på semester, kan det ge tjuven en perfekt möjlighet att slå till medan du är borta.
   Det kan absolut verka löjligt att tänka så och jag kan förstå dig. Men dom som vill göra skada, inbrott eller stjäla din identitet kommer ha det mycket enklare för sig när allt blir serverat på bordet. Fråga dig själv ifall du verkligen måste lägga ut en viss typ av information. Vad tjänar du på det?

Det är olika beteenden som kan hjälpa oss att bli säkrare online som i sin tur hjälper oss att tänka säkert och bli mer medvetna om konsekvenser över lag.

_02____Enkla lösningar som gör stor nytta

Det finns vissa åtgärder du kan ta för att öka din säkerhet. Vissa är mer tekniska men jag vill säga att stegen nedan är enkla att börja använda och implementera i sitt digitala liv.

Ibland är det enkelt men inte alltid självklart. I denna del berör vi inte bara säkerhet kring hur du kan skydda dig online utan också hur du kan skydda viktig information från att försvinna.

1. **Uppdateringar**: Att uppdatera mjukvara och hårdvara handlar inte bara om nya funktioner eller snabbare prestanda, utan också om att åtgärda sårbarheter som kan utnyttjas av angripare. En sårbarhet kan ge en angripare kontroll över din enhet, köra skadlig kod eller använda din enhet för att skada andra. Varje uppdatering innehåller information om vad som åtgärdas, och det är ofta enkelt att uppdatera eftersom du ofta får påminnelser om det i till exempel din telefon eller dator.

2. **Backup/säkerhetskopior:** Lita inte på att din enhet kommer fungera för alltid – ibland går prylar sönder och då kan viktig data förloras. Genom att ha en backup kan du undvika att förlora timmar av arbete, värdefulla familjefoton, viktiga dokument och anteckningar. Investera i en extern hårddisk eller en molntjänst som du känner dig trygg med för att spara kopior av din data, så att du alltid har en backup ifall något går fel.

3. **Multifaktorsautentisering**: En enkel lösning som du kommer väldigt långt med. Detta rekommenderas till alla att använda ihop med sina konton på olika plattformar. Idag erbjuder de flesta tjänster denna lösning vilket är kostnadsfritt och har stort inflytande på dina konton. Man kan använda sig av SMS, Autentiseringsapp (Google, Microsoft, Authy m.m.) vid inloggningstillfället. Det är ett extra lager av säkerhet och otroligt enkelt att börja använda. Det funkar genom att du får behöver verifiera dig en gång till när du loggar in och då använder du din autentiseringsapp eller får koden via SMS.
   Det är rekommenderat att använda annan metod än SMS pga säkerhetsskäl där man kan stjäla numret, men det är ändå bättre än ingen multifaktor alls!

_03____Bemästra säkerheten!

Har du kommit en bit på vägen så kan du lika gärna fortsätta! Förhoppningsvis ökar din medvetenhet med tiden och du bestämmer dig för att ha andra lösningar som kan både förenkla din vardag men samtidigt bidra till ökad säkerhet.

1. **Lösenordshanterare:** En lösenordshanterare underlättar genom att hjälpa dig skapa och lagra långa, komplexa lösenord, så att du slipper återanvända samma lösenord eller försöka minnas dem. Det finns många olika hanterare, alla med olika nivåer av kryptering och säkerhet. Jag rekommenderar Bitwarden, som fungerar som plugin i webbläsaren, app på telefonen och program på datorn, och som är kompatibel med Windows, MacOS och Linux. För mer information, besök Bitwardens hemsida.
   Andra populära alternativ inkluderar 1Password, Apple Keychain och Google Password Manager.
   **TIPS - Ladda även hem BitWarden Authenticator för att skydda ditt Bitwarden-konto med tvåfaktorsautentisering!*

2. **Krypterad kommunikation:** Jag använder krypterade meddelandetjänster när jag chattar med vänner och familj och rekommenderar Signal, en app som finns att ladda ner på dina enheter. Att kommunicera krypterat borde vara en självklarhet, särskilt när vissa samtal är privata och endast berör avsändaren och mottagaren. Det ger en extra trygghet att veta att dina konversationer är skyddade, och att du kan kommunicera säkert utan att oroa dig för att någon obehörig kan lyssna in. Användning av Signal innebär att du som skickar meddelande till dina kontakter skickar det krypterat där endast mottagaren kan “dekryptera” meddelandet. Det sker per automatik och inget du behöver aktivt göra.
   Flertalet myndigheter och underrättelsetjänster rekommenderar Signal.

3. **VPN**: I tidigare steg nämnde jag att använda VPN när du ansluter till publika nätverk. En VPN fungerar på det sätt att den skickar din datatrafik i en tunnel, krypterat till tjänstens servrar och skickas sedan vidare till slutdestinationen därifrån. Du gömmer dig helt enkelt bakom en vägg som ger dig ett extra skydd från din internetleverantör och från andra hemsidor som vill spåra geografisk plats, trafik och övrig spårning.
   Mullvad VPN är starkt rekommenderat och ett stort plus är att du kan betala kontant utan att registrera några uppgifter om dig.

PHATHACKZ

_04____Skydda dina personuppgifter!

I detta steg får du information om hur du kan minska eller ta bort dina personuppgifter från olika söktjänster. Tyvärr så får våra uppgifter hanteras av sökmotorer som hitta.se eller eniro.se. Där finns din adress, vilka du bor med, när du flyttat dit, löneuppgifter, tidigare domar m.m. tillgängligt för allihopa! Ta ett stort steg mot din integritet och dölj dina uppgifter.

1. **Dölj dina uppgifter online:** Du kan skydda dina personuppgifter från webbplatser som Ratsit.se, Hitta.se och Upplysning.se genom att välja att dölja eller helt ta bort din information. Vissa av dessa tjänster kräver att du verifierar dig med BankID för att hantera dina uppgifter. Genom att minska din synlighet i sökningar och begränsa tillgången till din information, kan du stärka ditt digitala skydd och minska risken för att dina uppgifter används på ett oönskat sätt online. För med information: https://nathatshjalpen.se/a/adress-telefonnummer-online

2. **Testa säkerheten på en hemsida:** Genom att använda detta steget så skyddar du dina personuppgifter *indirekt.* Säkerhetskollen har gjort en väldigt bra sajt där du kan skriva in och kontrollera en annan hemsida. Kanske ska du göra ett internetköp men är osäker på att knappa in dina uppgifter? I de flesta fall jag använt sidan så funkar den utmärkt till just detta!
   Ett mycket bra tips! Länken hittar du här: https://testa.sakerhetskollen.se/

3. **Kontrollera om dina uppgifter har varit med i en dataläcka:** Är du orolig att dina uppgifter har varit med i en läcka? Med denna tjänst får du väldigt bra insyn i tidigare dataläckor som fångats upp på nätet. Här kan du skriva in din e-postadress som tittar igenom databaser på läckor. Du ser vilka uppgifter som läckt (lösenord, namn, geografisk plats, kön m.m.) hos vilket företag och när det skedde. En bra indikator på att byta dina lösenord!
   Länken hittar du här: https://haveibeenpwned.com/

_05____Yttre skydd

Vad kan man ha för fysiskt skydd som också påverkar ens data egentligen?

1. **Kameraskydd:** Täck över din kamera på ett enkelt sätt! Antingen sätter du en tejpbit över kameran eller köper ett så kallat skydd för webbkameran som täcker över linsen men du kan enkelt dra skyddet åt andra sidan för att synas igen vid de tillfällen du har behov.
   Varför ska man skydda sin kamera? En angripare kan aktivera din kamera om du blivit utsatt för en attack. De kan i princip se i realtid eller ta foton utan att du som användare märker det. Detta är ett experiment jag själv har testat mot mig själv och mina egna enheter och det är skrämmande att man kan bli iakttagen i sitt hem när man surfar på datorn.

2. **Insynsskydd:** Idag finns det skärmskydd/insynsskydd man kan köpa till mobil och dator vilket innebär att du bara ser innehållet på din enhet om du håller den i en viss vinkel. Tittar du från sidan så ser man bara en svart skärm vilket är ett jättebra sätt att surfa lite tryggare utan att oroa sig för så kallad, “shoulder surfing”. Det finns flera typer av insynsskydd som skyddar olika mycket från olika vinklar. Det positiva med detta är att du även skyddar skärmen på din enhet med ett extra lager.

3. **Ta bort eller riv sönder kuvert, paket m.m:** Om du åker till en återvinningsplats kan du hitta paket, tidningar och paket med andras uppgifter på. Du kan hitta information om vad personen beställt, vart den bor, vad de betalat, ibland kan du hitta mailadresser, telefonnummer och annan information som du bör hålla för dig själv! Nästa gång du slänger post och paket, se till att riva sönder informationen om dig. Sannolikheten kanske inte är så stor att någon letar efter information men med tanke på hur lätt det blir att hitta information som tillhör dig utan att du vet om det är ganska obehagligt.

_06____Övriga tips

1. **Nerladdning av filer:** Det kan innebära en stor risk att ladda ner filer från internet. Ibland gör vi det från betrodda källor men ibland måste vi gå omvägar. Ett tips är att använda dig av tjänsten https://www.virustotal.com/, där du kan lägga in länken till filen eller ladda ner filen till din dator för att sen dra över installationsfilen till hemsidan. Denna tjänst skannar sedan av materialet och kör igenom flera antivirus-tjänster som letar efter skadlig kod.

2. **Val av webbläsare:** Med den snabba utvecklingen av Ai och hur data används idag av stora företag och tjänster så kan det vara smart att använda en webbläsare som fokuserar lite extra på integritet och säkerhet. Alla webbläsare har olika användarvillkor och din data hanteras, sälj eller skickas vidare beroende på vad för webbläsare du använder. Vad är det för data som webbläsare samlar in egentligen? Det beror på. Men det kan vara information om vart du surfar, vad du knappar in för uppgifter på olika hemsidor, vad du tittar på, vart du befinner dig, vilka tider du surfar på vilka saker. Tänk att i princip allt du gör så finns det en risk att den informationen finns lagrad någonstans.

PHATHACKZ

_07____0001x THE END

Jag hoppas att du haft nytta av detta häfte, vare sig du uppdaterar dina lösenord eller fått lite mer insikt på säkerheten online. Detta dokument kommer med tiden att utvecklas för att just du ska få tillgång till bra och enkla tips på hur du kan skydda dig på nätet. Utvecklingen går fort framåt och många lösningar skjuts över till internet och med det ökar vår sårbarhet.

Trots noggrann granskning kan felaktigheter, stavfel eller föråldrad information förekomma. Du som användare uppmanas att självständigt verifiera viktiga uppgifter. Jag tar inget ansvar för eventuella konsekvenser som kan uppstå vid användning av tips eller råd som ges här. Användningen av informationen sker på egen risk.

- SIGNERAT FATMIR NEZIRAJ // www.PHATHACKZ.se