



BETALNINGSHJÄLPEN

Trygghet och
säkerhet

Inledning

I dagens samhälle har internet blivit en central del av vår vardag, en resurs som erbjuder en oändlig mängd information och möjligheter för kommunikation och lärande. För de som inte är födda in i den digitala eran, kan det dock vara en utmaning att navigera i denna nya värld. Det är därför vi har skapat det här utbildningsmaterialet där du kan få kunskap och förståelse för att använda internet med säkerhet och självförtroende.

Vi kommer att börja med att diskutera vikten av att skydda din personliga information, en resurs som är lika värdefull online som den är i den fysiska världen.

Därefter kommer vi att utforska olika typer av online-bedrägerier och hur du kan känna igen och undvika dem. Detta är en viktig färdighet att ha, likt att kunna känna igen och undvika potentiella faror i den fysiska världen. Vi kommer att ge dig tips och råd om hur du kan genomföra säkra köp på nätet, så att du tryggt kan handla och utföra andra aktiviteter på nätet.

Slutligen kommer vi att mer ingående prata om hur du skapar och underhåller starka lösenord, en nyckelkomponent i att skydda din identitet på nätet. Vi kommer att ge dig råd om hur du kan använda modern teknik, inklusive biometrisk säkerhet, för att ytterligare stärka din online-säkerhet.

Det här utbildningsmaterialet är en grund för att börja navigera på internet med förtroende och säkerhet. Men kom ihåg att den digitala världen är i ständig förändring, med nya teknologier, tjänster och säkerhetshot som dyker upp regelbundet. Därför är det viktigt att inte bara rusta dig med kunskap och verktyg för stunden utan att fortsätta utbilda dig och hålla dig uppdaterad. Betalningshjälpen är här för att stödja dig på din digitala resa och uppmuntrar dig att regelbundet friska upp och utöka dina kunskaper. På så sätt kan du fortsätta vara en säker och kompetent internetanvändare, redo att möta framtidens utmaningar och möjligheter med tillförsikt.

Diskutera frågorna
tillsammans med
en vän!

Diskutera

- Varför tror ni att det är viktigt att förstå och känna sig trygg med internetanvändning, särskilt för de som inte växte upp med tekniken?
- Vilka är några av de största farhågorna ni har när det gäller att använda internet?



Skydda din personliga information

1. Användning av starka och unika lösenord

Starka och unika lösenord är viktiga för att skydda dina konton från obehörig åtkomst. Det minskar risken för identitetsstöld och andra former av cyberbrott.

Liknelse: Tänk på ditt lösenord som en nyckel till ett säkert kassaskåp där du förvarar dina mest värdefulla tillhörigheter. Varje nyckel bör vara unik och komplex för att förhindra obehörig åtkomst.

2. Tvåfaktorsautentisering

Tvåfaktorsautentisering är en säkerhetsprocess där användaren måste tillhandahålla två olika sätt för att verifiera sin identitet. Ett vanligt sätt är att använda SMS som ett tillägg till namn och lösenord. När du loggar in på en tjänst, skickas också en engångskod via SMS till din mobiltelefon. Du måste ange denna kod för att slutföra inloggningen. Detta kan användas till exempel med banktjänster, e-post, sociala medier och offentliga tjänster.

Liknelse: Detta är som att ha dubbla lås på din dörr; även om någon har din ena nyckel, kan de inte komma in utan den andra nyckeln.

3. Hantering av personlig information

Var försiktig med vilken information du delar online. I Sverige är en del personlig information som hemadress och telefonnummer offentliga på grund av offentlighetsprincipen. Trots detta är det viktigt att vara medveten om vilken information du delar på sociala medier och andra offentliga forum.

Undvik till exempel att offentligt dela personnummer, bankuppgifter eller bilder och statusuppdateringar som berättar att du är på semester.

Liknelse: Dela din personliga information med samma försiktighet som du skulle dela en familjehemlighet.

Diskutera

- Hur kan betalningar på nätet göra livet enklare?
- Vad gör ni för att känna er trygga när ni betalar på nätet?



Undvika bedrägerier och fällor



1. Phishing

Phishing är ett försök att få känslig information såsom användarnamn, lösenord och kreditkortsdetaljer genom att utge sig för att vara en pålitlig avsändare i en elektronisk kommunikation.

Liknelse: Phishing-försök är som falska försäljare som försöker lura dig att köpa något du inte behöver eller vill ha.

Tips:

Var försiktig med e-postmeddelanden eller meddelanden som begär personlig information eller hänvisar till en webbplats med okända länkar. Kontrollera avsändarens e-postadress och var uppmärksam mot stavfel eller konstiga formuleringar.



2. Spoofing

Spoofing är en metod där bedragare förfalskar identiteter - som telefonnummer eller e-postadresser - för att få det att verka som om de är någon du känner och litar på.

Liknelse: Tänk på spoofing som en bedragare som klär ut sig till en vän eller en officiell person för att vinna ditt förtroende och sedan utnyttja det.

Tips:

Om du får ett oväntat samtal eller meddelande som ber om personlig information eller uppmanar dig att vidta åtgärder, var skeptisk.

Ett effektivt sätt att avslöja en spoofing-försök är att erbjuda att ringa upp personen eller organisationen direkt. Lägg på luren först och ring sedan tillbaka till ett nummer du vet är korrekt. Detta säkerställer att du faktiskt talar med den rätta personen och inte en bedragare som försöker lura dig.

Kom ihåg att ingen legitim organisation kommer att be dig om dina lösenord eller PIN-koder via telefon eller e-post.

3. Onlinebedrägerier

Det finns flera sätt som bedragare kan försöka lura dig på nätet, några vanliga är:

Lotteribedrägerier: Du får ett e-brev om att du vunnit i ett okänt lotteri och ombeds betala en avgift. Detta är oftast en bluff. Om du inte köpt en lott, har du inte vunnit.

Förmånstagarbedrägerier: Du får ett e-brev från någon som vill flytta stora pengar och behöver din hjälp. De ber dig betala en liten avgift med löfte om att du sedan kommer få tillbaka mycket mer.

Nätdejtingbedrägerier: Du träffar någon online som snabbt uttrycker starka känslor och ber om pengar. Ge aldrig ut pengar till någon på nätet, speciellt inte till någon du aldrig träffat i verkligheten.

Välgörenhetsbedrägeri: Efter stora naturkatastrofer och liknande skapar bedragare falska hemsidor där du kan bli uppmanad att skänka pengar. Kontrollera alltid webbplatsens äkthet innan du donerar.

Reparationsbedrägerier: Du får ett samtal från någon som påstår sig kunna hjälpa med din dator. De tar sedan över din dator med skadlig kod. Var försiktig med oömbdda teknikhjälpssamtal.

Liknelse: Onlinebedrägerier är helt enkelt moderna versioner av svindlare som använder digitala medel för att lura dig.

Tips:

Om du misstänker att du har blivit utsatt för ett bedrägeri, rapportera det till lokala myndigheter och varna dina vänner och familj för att undvika att de också blir lurade.

4. Säker handel på nätet

När du handlar online, se till att webbplatsen är säker (adressen bör börja med "https"). Kontrollera också att webbplatsen har goda recensioner och goda omdömen. Hör gärna med vänner och bekanta om de känner till hemsidan du vill handla från.

Liknelse: Tänk på säker näthandel som att handla i en välrenommerad butik i stället för på en tvivelaktig marknadsplats.

Tips:

Var försiktig med att dela ditt kreditkortsnummer och andra personliga uppgifter på hemsidor som verkar oseriösa. Använd alltid säkra, beprövade betalningsmetoder.

Ett enkelt sätt att se att webbplatsen är säker är att kolla om webbadressen börjar med "https".



Diskutera frågorna tillsammans med en vän!

Diskutera

- Har någon av er någonsin stött på ett phishing-försök? Hur kände ni igen det?
- Vilka är några varningssignaler ni letar efter för att identifiera en potentiell bluffwebbplats?
- Hur kan man bäst utbilda andra om riskerna med onlinebedrägerier?

Mer om säkra lösenord

Saker-81!losen

Niklas74

Vilket lösenord ovan tror du är det starkaste?

1. Skapa starka lösenord

Skapa lösenord som är minst 12 tecken långa och innehåller en blandning av bokstäver, siffror och specialtecken. Undvik att använda uppenbara ord eller fraser som ditt namn, året du är född och liknande.

2. Använd en lösenordshanterare

En lösenordshanterare är ett program som skapar, lagrar och hanterar dina lösenord för olika webbplatser och appar. Tänk på det som ett digitalt kassaskåp där dina lösenord är tryggt förvarade bakom ett enda, viktigt lösenord – det enda du behöver komma ihåg. Lösenordshanterare hjälper också till att skapa starka och unika lösenord för varje konto, vilket avsevärt minskar risken för digitalt intrång. I en lösenordshanterare är dina lösenord krypterade för maximal säkerhet. Populära exempel är NordPass, 1Password, och Bitwarden. Du skaffar dem enklast genom att ladda hem dem från respektive hemsida.

3. Uppdatera lösenord löpande

Genom att regelbundet uppdatera dina lösenord minskar du risken för att någon ska få obehörig åtkomst till dina konton. För bästa säkerhet rekommenderas det att du ändrar dina lösenord var tredje till sjätte månad. Dessutom är det viktigt att komma ihåg att inte återanvända gamla lösenord. Säkerhet bör alltid vara en prioritet, och med dessa enkla steg kan du hålla dina digitala dörrar låsta och säkra.

4. Användning av biometrisk säkerhet

Biometrisk säkerhet handlar om att använda dina unika kännetecken, som ditt fingeravtryck eller ditt ansikte, för att bekräfta din identitet. Många moderna enheter som mobiltelefoner, erbjuder denna typ av säkerhetsfunktion. Tänk på biometrisk säkerhet som en personlig nyckel som endast fungerar för dig, vilket gör det både enkelt och säkert att skydda din information.



För bästa säkerhet rekommenderas det att du ändrar dina lösenord var tredje till sjätte månad.

Diskutera frågorna
tillsammans med
en vän!

Diskutera

- Hur ofta ändrar ni era lösenord? Använder ni samma lösenord för flera konton?
- Vad tycker ni om idén att använda en lösenordshanterare? Ser ni några potentiella risker med det?
- Hur känner ni för att använda biometrisk säkerhet, som fingeravtryck eller ansiktsgenkänning, för att skydda era enheter och konton?



Sammanfattning

När vi navigerar på internet, lämnar vi spår bakom oss som tillsammans bildar vårt "digitala fotavtryck". Detta kan inkludera information som vi medvetet delar, såsom inlägg på sociala medier, samt data som samlas in av webbplatser vi besöker, såsom vår plats- eller sökhistorik. Det är viktigt att vara medveten om vilken typ av information vi delar online och att hantera sitt digitala fotavtryck på ett säkert och ansvarsfullt sätt.

Kom ihåg att alltid vara vaksam och ta de nödvändiga försiktighetsåtgärderna för att skydda dig själv online. Det är viktigt att hålla sig uppdaterad med de senaste säkerhetstipsen och att vara proaktiv i att skydda din personliga information.

Men när du delar, interagerar och lär dig online, gör det med glädje och nyfikenhet. Internet är en plattform där du kan upptäcka, skapa och hålla kontakten på sätt som var otänkbara för bara några årtionden sedan. Så ta vara på dessa möjligheter och låt din digitala resa bli en källa till berikande erfarenheter och positiva bidrag till den värld vi alla delar.



Diskutera frågorna
tillsammans med
en vän!

Diskutera

- Vad menas med ett "digitalt fotavtryck"? Hur kan vi bäst hantera och skydda vårt digitala fotavtryck?
- Vilka steg kommer ni att ta efter den här sessionen för att förbättra er online-säkerhet?

