SKPF Pensionärerna
Utbildningsmaterial

TRYGGHET OCH SÄKERHET
EN BRA INVESTERING

Trygga Tips

Bedrägerier och digital säkerhet

SKPF pensionärerna

Innehållsförteckning

Introduktion

Välkommen till Trygga Tips – din guide till en tryggare vardag. Dessa tips är skapade för att hjälpa dig att öka din medvetenhet om säkerhetsfrågor och ge praktiska råd för att förebygga risker.

Vårt mål är att du ska känna dig säker i alla aspekter av ditt liv, från hemmets trygga vrå till den digitala världen.

Varje kapitel innehåller praktiska råd, tips och länkar för att du ska kunna använda kunskapen direkt i din vardag.

Kom ihåg!

• Du har ett eget ansvar. Du har kraften att påverka din egen säkerhet genom att vara medveten och vidta förebyggande åtgärder.

• Samverka med samhället omkring dig. Tillsammans med familj, vänner och SKPF Pensionärerna kan vi skapa ett tryggare samhälle.

Bedrägerier

Anmäl alla brott till polisen. Bedragare har alltid funnits genom tiderna. Genom alla tider har människor försökt utnyttja andra för egen vinning. I dag är digitala medier en ytterligare arena för bedrägerier. Genom internet och sociala plattformar kan bedragare nå ut till fler människor än någonsin tidigare, och deras metoder blir alltmer sofistikerade. Här är exempel:

Nätfiske (Phishing)

Bedragare skickar falska e-postmeddelanden som ser ut att komma från pålitliga källor som banker eller myndigheter. De försöker lura dig att avslöja personlig information som lösenord och kontonummer eller få dig att logga in på din bank och föra över dina pengar till någon annan.

Identitetsstöld

Om någon får tillgång till dina personuppgifter kan de använda dem för att öppna kreditkonton, ta lån, ändra din adress eller göra köp i ditt namn. På Skatteverket kan du spärra obehörig adressändring. Använd tjänsten ”Spärra obehörig adressändring” om du vill att dina adressanmälningar hos Skatteverket ska göras med e-legitimation och inte på pappersblankett.

Falska meddelanden

Bluff-sms eller telefonsamtal som verkar komma från betrodda organisationer kan be dig att uppge känslig information eller ringa ett nummer för att ”lösa ett problem” med ditt konto, klicka på länkar eller göra betalningar. Anmäl misstänkta bluff-sms genom att vidarebefordra meddelandet till 7726. Siffrorna motsvarar ordet SPAM på knappsatsen på telefonen och är globalt etablerat för att rapportera bluff-sms. Det är ett operatörsoberoende nummer så att alla kan använda det.

Romansbedrägerier

Innebär att någon på internet låtsas vara intresserad av en romantisk relation för att utnyttja dig ekonomiskt eller på andra sätt. Bedragaren kan använda falska profiler på sociala medier, dejtingsajter eller via e-post och sms.

Investeringsbedrägerier

Dessa involverar orealistiska erbjudanden och löften om höga avkastningar på investeringar med liten eller ingen risk. Bedragarna pressar för snabba beslut och skapar en känsla av brådska för att du inte ska hinna tänka efter eller rådfråga någon.

Lotteri- och prisbedrägerier

Du får meddelanden om att du har vunnit ett lotteri eller en tävling du inte har deltagit i. De ber om en betalning för att du ska kunna ta emot priset, vilket är ett tydligt varningstecken på bedrägeri.

Bedragare försöker lura sig in i din bostad

• Bedragare utger sig för att vara hantverkare eller fastighetsskötare som ska kontrollera något i bostaden.

• Bedragare utger sig för att komma från hemvården, sjukvården, ett säkerhetsföretag, polisen eller annan myndighet.

• Bedragare låtsas vilja sälja en tjänst, en vara eller ber om att få låna toaletten.

• Bedragare låtsas att de vill lämna ett meddelande till någon av dina grannar som inte är hemma.

• Bedragaren påstår sig vilja skydda dina värdesaker och fotografera dem åt dig. Bedragaren säger även att du senare kommer att få tillbaka värdesakerna, vilket du aldrig får.

Lägenhetsbedrägerier

Bostadsbristen utnyttjas av bedragare som utger sig för att vara mäklare eller fastighetsägare som lurar människor med falska lägenhetsannonser. Bedragare kopierar ofta bostadsrättsannonser och gör om dem till andrahandsannonser.

Om hyresvärden kräver förskottsbetalning innan du ens sett lägenheten, bör du vara misstänksam. Begär legitimation. Kontrollera att lägenheten existerar. Besök alltid lägenheten innan du betalar något. Kontrollera adressen, mäklaren och fastighetsägaren. Undvik att betala via anonyma betalningstjänster eller kontanter.

Fastighetsmäklarinspektionen, FMI är en statlig myndighet som ansvarar för registrering och tillsyn av fastighetsmäklare och fastighetsmäklarföretag.

Organiserad brottslighet och hemtjänst

Sedan 2019 krävs det tillstånd från Inspektionen för vård och omsorg, IVO, för att bedriva hemtjänst. Trots detta har IVO funnit ett antal bolag som saknar tillstånd och som inte heller har sökt tillstånd, men som ändå utfört hemtjänst.

Kontakta din kommuns biståndshandläggare om du har frågor eller behöver hjälp att ansöka om insatser inom vård och omsorg.

Var uppmärksam på:

• Ovanligt låga priser: Om ett erbjudande verkar för bra för att vara sant, är det ofta det. Kriminella kan locka med mycket låga priser för att snabbt få tillgång till dina pengar eller ditt hem.

• Svårkontaktade företag: Om företaget är svårt att nå på telefon, undviker skriftlig kommunikation eller saknar en fysisk adress – se upp!

• Otydligt ansvar: Seriösa aktörer har tydliga rutiner, tydlig prissättning och villkor. Kriminella kan vara vaga eller motsägande när du ställer frågor.

• Be om legitimation: Begär alltid att representanter från hemtjänstföretaget uppvisar giltig legitimation. Det är helt OK att notera namn och personnummer.

Oseriösa hantverkare

Bedragare kan erbjuda billiga husrenoveringar eller asfaltering av uppfarten, men levererar dåligt arbete eller inget alls. Om någon dyker upp oanmäld och erbjuder tjänster till ett ovanligt lågt pris, bör du vara försiktig.

Oseriösa hantverkare undviker ofta skriftliga avtal och kvitton. Anlita seriösa hantverkare och ha ett skriftligt avtal som specificerar arbete, kostnad och tidsram. Kontrollera att hantverkaren är registrerad och har F-skattesedel. Det gör du hos Skatteverket.

Utpressningsvirus (Ransomware)

Utpressningsvirus är skadlig programvara som låser din dator eller krypterar filer och kräver en lösensumma för att återställa dem.

Var uppmärksam på

• Misstänkta e-postmeddelanden eftersom viruset sprids ofta via e-post med bifogade filer eller länkar.

• Pop-up-meddelanden med varningar som säger att din dator är infekterad och att du måste betala för att åtgärda det.

• Skydda dig genom att säkerhetskopiera din dator eller telefon regelbundet. Ha alltid en uppdaterad backup av dina viktiga filer på en extern enhet eller i molnet – på exempelvis Microsoft OneDrive (PC) eller Apple iCloud (Mac).

• Installera antivirusprogram och håll det uppdaterat.

Om du drabbas

• Koppla omedelbart bort den drabbade datorn från nätverket, oavsett om det är trådlöst eller med sladd, men stäng inte av datorn eftersom i vissa fall kan innebära att installation av den skadliga koden slutförs.

• Byt lösenord för alla drabbade konton, framför allt administratörskonton.

• Betala inte lösensumman och anmäl attacken till polisen. Att betala garanterar inte att du får tillbaka dina filer.

• Installera om datorn, uppdatera din antivirusprogramvara och genomför en ny sökning av den nyinstallerade datorn.

Köp med kontokort

Bedragare kan försöka stjäla dina kortuppgifter genom olika metoder vid bankomater och kassor.

Var uppmärksam på:

• Personer som står för nära och försöker se din PIN-kod över axeln.

• Bedragare kan försöka distrahera dig genom att tappa en sedel, fråga om vägen eller smeta något på dig.

Hur du skyddar dig

• Täck över tangentbordet när du slår in din PIN-kod och var vaksam på omgivningen.

• Om någon står för nära, be personen att backa eller låt dem gå före dig i kön.

• Känner du dig osäker eller obekväm, avbryt transaktionen.

• Ha inte kort och pengar i lättillgängliga fickor eller öppna väskor.

Säkerhetsåtgärder

• Var skeptisk. Lita inte blint på alla meddelanden eller samtal. Om något känns fel, undersök saken närmare.

• Kontrollera källan. Om du blir kontaktad av din bank eller en myndighet, ring tillbaka på ett nummer du vet är korrekt för att verifiera äktheten.

• Klicka inte på misstänkta länkar. Öppna inte länkar eller bilagor från okända eller misstänkta avsändare.

• Uppdatera dina programvaror och appar. Håll din dator och dina enheter uppdaterade med den senaste programvaran.

• Dela inte känslig information. Ge inte ut personnummer, bankuppgifter eller lösenord till någon som kontaktar dig oväntat.

• Använd starka lösenord. Kombinera bokstäver, meningar, siffror och specialtecken, och använd olika lösenord för olika tjänster.

• Använd en lösenordshanterare i din dator eller telefon för att skapa och säkert förvara dina lösenord.

• Aktivera tvåfaktorsautentisering. Tvåfaktorsautentisering (2FA) är en säkerhetsmetod som kräver två olika typer av verifiering för att bekräfta din identitet. Den är säkrare än bara ett lösenord.

2FA bygger på principen att kombinera något du vet (till exempel ett lösenord) med något du har (till exempel en mobilapp, SMS-kod eller säkerhetsnyckel) eller något du är (till exempel fingeravtryck eller ansiktsigenkänning). Detta gör det svårare för obehöriga att få tillgång till ett konto, även om de lyckas stjäla lösenordet.

• Använd betalkort med säkerhetsfunktioner.

• Föredra betaltjänster som Swish.

• Betala inte i förväg till okända säljare.

• Kontrollera regelbundet dina kontoutdrag.

• Anmäl omedelbart misstänkta transaktioner till din bank.

Om du misstänker ett bedrägeri

• Avbryt kontakten. Svara inte på misstänkta meddelanden eller samtal. Lägg på luren.

• Anmäl händelsen. Kontakta polisen och rapportera bedrägeriet.

• Informera berörda organisationer. Om dina bankuppgifter kan ha kompromitterats, kontakta omedelbart din bank.

• Var öppen med nära och kära. Berätta för familj eller vänner om vad som hänt så att de också kan vara uppmärksamma.

Kom ihåg

Skäms inte. Du är inte ensam. Många har drabbats av bedrägerier, och det är inget att skämmas över. Sök stöd. Om du känner dig upprörd eller orolig efter en sådan upplevelse, tveka inte att söka stöd från vänner, familj eller professionella.

Länkar

Apple iCloud – säkerhetskopiering i molnet (Mac):
www.icloud.com

Fastighetsmäklarinspektionen:
www.fmi.se

Finansinspektionen – FI är en statlig myndighet med uppgift att övervaka finansmarknaden:
www.fi.se

Hallå Konsument – vägledning för konsumenter:
www.hallakonsument.se

IVO – Inspektionen för vård och omsorg:
www.ivo.se

Konsumentverket:
www.konsumentverket.se

Lantmäteriet – vem äger fastigheten:
www.lantmateriet.se

Microsoft OneDrive – säkerhetskopiering i molnet (PC):
www.microsoft.com

Polisen:
www.polisen.se

Skatteverket – spärra obehörig adressändring, kontrollera F-skatt:
www.skatteverket.se

Säkerhetskollen – fördjupa dig i digital säkerhet, råd vid utpressningsvirus:

www.sakerhetskollen.se

Anteckningar

SKPF
pensionärerna

Sveavägen 68, Box 3619, 103 59 Stockholm
010-222 81 00 • info@skpf.se • www.skpf.se