Ekspert: KI-svindel skal bekjempes med KI

Chief Strategy Officer ved sikkerhetsselskapet Syndis, David Jacoby, forteller til Komputer for alle at kunstig intelligens er i full gang med å endre sikkerheten på nettet. Det gjelder for både angripere og forsvarere. KI kan gjør svindelforsøkene langt mer overbevisende, men David Jacoby forteller at KI også kan styrke forsvaret. Kunstig intelligens brukes nemlig i økende grad til å oppdage uregelmessigheter i nettverkstrafikk, markere suspekte transaksjoner i sanntid, oppdage deepfake-innhold og automatisere håndtering av hendelser. Rustningskappløpet gjør også de kriminelle mer kreative, men sikkerhetssystemene tilpasser seg, og det skjer ofte ved hjelp av den samme teknologien. Resultatet er avhengig av i hvilken grad defensiv KI klarer å ligge et hestehode foran angriperne. Kunnskap, flerfaktorgodkjenning og KI-drevet, sanntids trusseloppdagelse er avgjørende.

David Jacoby, Chief Strategy Officer, Syndis.

Foto: Skorzewiak/Shutterstock.com

NYTT ÅR – NYE TRUSLER:

Slik vil IT-kriminelle angripe i 2026

Året som ligger foran oss, byr på flere sikkerhetsutfordringer. Nye trusler er under oppseiling, og angrepene blir stadig mer krevende å avsløre.

Journalist
Henning Rasmussen

Tidlig en søndag morgen ringer telefonen. Du gjenkjenner øyeblikkelig stemmen til barnebarnet, som fortvilet forklarer at han har vært innblandet i en trafikkulykke. Nesen er brukket, og han har sterke smerter. I forbindelse med ulykken er han arrestert av politiet, og ber nå om at du raskt overfører noen tusen kroner for å dekke det mest nødvendige mens han er i politiets varetekt.

KI-svindel på fremmarsj

Det kan høres ut som en besteforelders verste mareritt. I virkeligheten er det snakk om et utspekulert svindelforsøk. Stemmen til barnebarnet er generert av kunstig intelligens, og folkene bak oppringningen er noen dyktige svindlere som bare er ute etter pengene dine. Eksempelet med barnebarnet virker kanskje oppdiktet, men dette var faktisk nøyaktig det den 73 år gamle kanadiske Ruth Card ble utsatt for.

Historien hennes er gjengitt i den amerikanske storavisen Washington Post. Der fremgår det også at Ruth Card rakk å ta ut over 20 000 kroner til svindlerne, før en bankansatt trakk den eldre damen til side og advarte om at en annen av bankens kunder for kort tid siden var blitt lurt av den samme svindelmetoden.

På rekordtid har kunstig intelligens spredd seg til alle tenkelige tjenester og verktøy. Det betyr at KI også er tatt i bruk av svindlere som kan gjennomføre større, billigere og mer overbevisende aksjoner.

I det nevnte tilfellet med å etterligne stemmen til en pårørende, er det nok med noen få setninger for å få den kunstige intelligensen til å kopiere stemmen. Stemmeprøven kan hentes fra en YouTube-video eller et annet klipp fra sosiale medier som er fritt tilgjengelig på nettet. Det krever heller ikke noen stor teknisk innsikt å gjennomføre svindelen. KI-verktøy som kan etterligne stemmer, er nemlig også fritt tilgjengelig på nettet sammen med en rekke andre verktøy som kan misbrukes av uærlige sjeler. Det gjelder blant annet ElevenLabs, som også brukes til svindel. Tjenesten er en kunstig intelligens som kan generere falske stemmer, og som tidligere har blitt kritisert for å få for eksempel Harry Potter-skuespiller Emma Watson til å sitere fra Hitlers "Mein Kampf."

Stadig mer overbevisende

Den store utfordringen i året som kommer, er at det blir mer krevende å avsløre KI-baserte svindelforsøk, og at den svært troverdige svindelen gjør seg gjeldende på alle plattformer. Du må altså være forberedt på at du kan bli forsøkt lurt både via telefonsamtaler, tekstmeldinger og e-post, og at du alltid må være på vakt når du bruker ulike former for elektronisk kommunikasjon. Svindel kan forekomme i både apper, på nettsider og i annonser på sosiale medier.

I denne artikkelen kan du lese mer om truslene du bør være mest oppmerksom på i tiden fremover.

Svindlerne kan benytte seg av gratisverktøy på nettet eller pc-programmer som DeepFaceLab til å lage falske videoer som er så realistiske at de kan lure ofrene til å tro på det personene i videoene forteller.

En overhengende KI-trussel

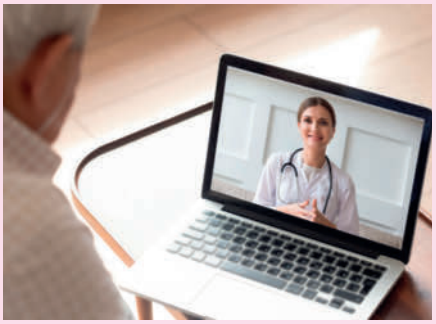
Hackere har forlengst tatt i bruk kunstig intelligens til å lage mer troverdige angrep. Det krever nye vaner fra de potensielle ofrene – altså oss alle.

Kunstig intelligens har for alvor funnet veien til hackernes verktøykasse. Ved hjelp av KI kan kyberkriminelle skreddersy e-postmeldinger som er både grammatisk korrekte og skreddersydd for deg og din situasjon.

Ifølge IBMs X-Force-rapport fra 2024 blir opptil 60 prosent av disse KI-genererte forsøkene på nettfiske via e-post åpnet, fordi de til forveksling ligner legitime henvendelser. En annen økende trussel er den utbredte bruken

HVORDAN SIKRE SEG

Det kan være vanskelig å holde hodet kaldt når man befinner seg i en situasjon der man får telefon eller en tekstmelding fra en nærstående i knipe. Det gjør det enda vanskeligere å avsløre det, hvis det er snakk om svindel. Derfor anbefaler de fleste eksperter at man internt i den nærmeste familien allerede nå blir enige om et hemmelig passord eller en hemmelig setning som ingen andre kjenner til. Dermed vet du raskt om de som kontakter deg er blant de nærmeste – eller om det er svindel.



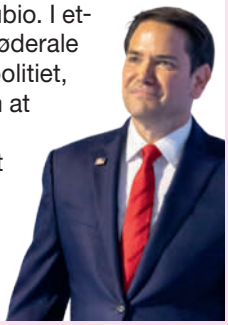
Du skal ikke tro på alt du ser eller leser på nettet. I senere år har kjente mennesker blitt misbrukt til svindel, for eksempel for å lure deg til å investere i falsk kryptovaluta. Du bør også være på vakt hvis du blir kontaktet av banken eller sykehuset.

De fleste blir bekymret og er på tilbudssiden hvis noen fra banken eller en nær slektning ringer med foruroligende nyheter. Før du reagerer på informasjonen, bør du forsikre deg om at vedkommende i den andre enden er den hen gir seg ut for å være.

Foto: fizkes, Prostock-studio, Tero Vesalainen, Tada Images, Arkhipenko Olga/Shutterstock.com

Falsk stemme etterlignet utenriksminister

I sommermånedene i 2025 sendte det amerikanske utenrigsdepartementet, US Department of State, en advarsel til landets utenlandske diplomater. Svindlere hadde brukt kunstig intelligens til å skape falske stemmeopptak av utenriksminister Marco Rubio. Disse opptakene ble deretter brukt til å kontakte tre utenriksministre i andre lande, en amerikansk senator og en amerikansk guvernør. Svindlerne hadde altså klart å bruke KI tli å kontakte de forskjellige personene via tjenesten Signal med tekst- og talemeldinger med en stemme som hørtes ut som Marco Rubio. I ettertid har det føderale amerikanske politiet, FBI, advart om at denne formen for KI-generert svindel er et økende problem i rask fremgang.

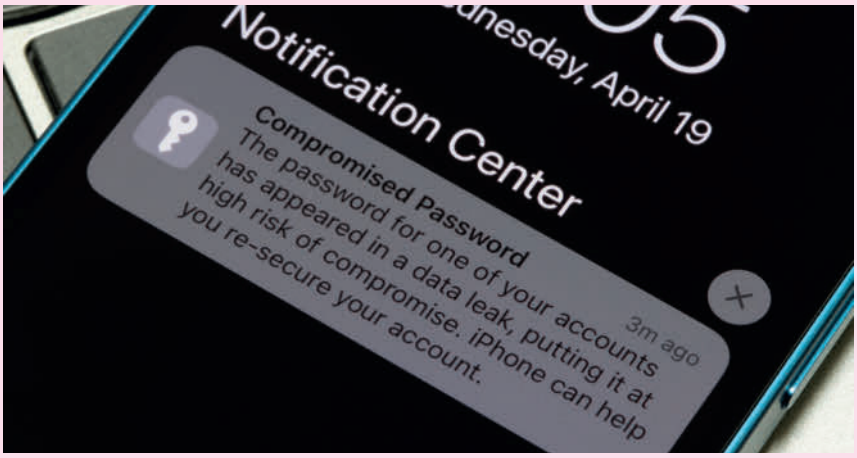


av såkalt deepfake-teknologi der stemmer og video kan etterlignes til minste detalj.

En rekke tilfeller har vist hvordan svindlere med klonede stemmer har ringt til ulike selskaper og utgitt seg for å være sjefen eller lederen av regnskapsavdelingen. I et eksempel publisert av nyhetsbyrået AP News ble en amerikansk politiker klonet for å narre folk i embetsverket.

Samtidig bruker hackere KI til å finne sikkerhetshull i programmer og systemer før utvikleren rekker å tette det (såkalt nulldagssårbarhet), mye raskere enn tidligere.

Ifølge Computer Science and Artificial Intelligence Laboratory ved MIT kan hele angrepsplanen automatiseres med språkmodeller, slik at selv uerfarne hackere kan gjøre stor skade. Derfor må også dine sikkerhetsrutiner holde tritt med utviklingen.



På en iPhone blir du advart hvis et passord du bruker har dukket opp i en datalekkasje. Du kan aktivere den samme beskyttelsen på Google-kontoen, eller få vist den på pc-skjermen ved hjelp av programmet HackCheck.

Tjenester hackes

En datalekkasje betyr at passord, kortopplysninger og private data kan havne i feil hender.

Har du konto på en nettjeneste som blir hacket, kan også din informasjon bli del av en såkalt datalekkasje. Det kan innebære at brukernavn, passord og noen ganger også betalingsinformasjon kommer på avveie og selges videre. Ifølge analysefirmaet Surfshark ble over 300 millioner kontoer lekket bare i 2023.

Du oppdager det kanskje først når det plutselig trekkes penger fra kontoen eller noen logger inn på din konto i ditt navn, og begynner å dele eller sende ting med deg som avsender. Ifølge Stanford University skjer de fleste identitetstyverier som følge av nettopp datalekkasjer, og det kan ramme selv om du ikke umiddelbart har gjort noe galt.

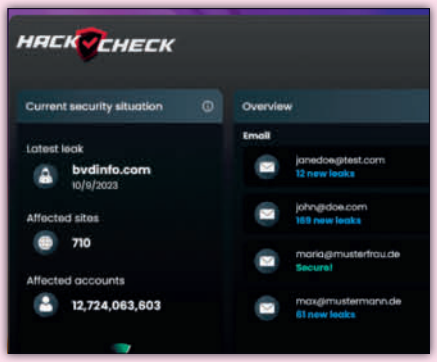
Informasjonen din kan nemlig bli stjålet via tjenester du har brukt i årevis, fra nettbutikker til e-postsystemer, og misbruket kan pågå i lang tid før det blir oppdaget.

Derfor er det så viktig å ha ulike passord til alle tjenester du benytter, og at du aktiverer tofaktorautentisering der det er mulig. Det gjør det mye vanskeligere for en hacker å utnytte dine data hvis uhellet er ute.

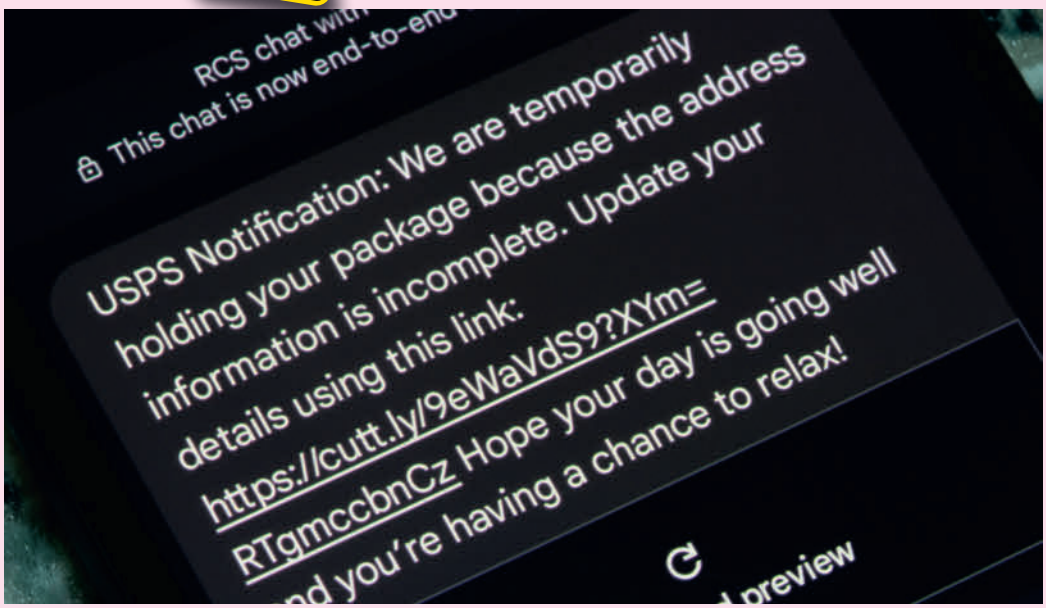
HVORDAN SIKRE SEG

På siden haveibeenpwned.com kan du oppgi e-postadressen din og umiddelbart få vite om den har kommet på avveie i en datalekkasje. Hvis du installerer programmet Abelssoft HackCheck på maskinen, kan du også bli varslet automatisk. Da vises en advarsel på Windows-skrivebordet hvis den tilknyttede kontoen er i fare.

Programmet ligger på **komputer.no/2520**



Abelssoft HackCheck, som du kan laste ned fra nettsiden vår, ligger i bakgrunnen på Windows-maskinen og viser en advarsel hvis en av e-postadressene dine har vært involvert i et datalekkasje.



Du kan få melding om en pakke som først kan utleveres etter at du har betalt et mindre gebyr. Meldingen må ikke nødvendigvis være på norsk.

Svindlerne blir stadig flinkere til å lure oss

Nettfiske via e-post og sms ("smishing") er svindelmetoder der noen prøver å få deg til å oppgi fortrolig informasjon ved hjelp av tilforlatelige meldinger.

Dagens kriminelle utvikler seg i takt med teknologien. Det gjør det krevende å skulle skille mellom ekte og falske meldinger. Nettfiske ("phishing") foregår typisk via e-post, mens "smishing" sendes til mobilen som sms. Begge har samme formål, nemlig å få deg til å klikke på en kobling eller oppgi personlig informasjon. Slike meldinger ligner til forveksling en melding fra en bank, en frakttjeneste eller en offentlig institusjon.

Klikker du på koblingen som er satt inn, kan du ende med å gi svindlerne tilgang til å heve penger med dine betalingskort eller å logge inn på tjenester du benytter.

Ifølge Europol blir denne svindelformen langt mer avansert for hvert år som går, og kunstig intelligens brukes nå rutinemessig av kriminelle til å formulere svindelmeldinger på perfekt norsk.

Sunn skepsis er ditt beste forsvar. Klikk aldri på koblinger i uoppfordret e-post eller meldinger. Bare slett den, hvis avsenderen er ukjent.

HVORDAN SIKRE SEG

De falske meldingene gjør ikke i seg selv skade på verken mobil eller pc. Skaden skjer først hvis du følger de falske anvisningene i meldingene og for eksempel klikker på en kobling eller oppgir følsom informasjon. Det beste middelet mot svindelen er derfor å ganske enkelt slette de falske meldingene, og i hvert fall la være å følge koblingen(e) i meldingen.

Når du får melding fra et frakt-selskap, banken eller en offentlig institusjon og er i tvil om den er ekte, skal du ikke reagere på meldingen. Ring i stedet det ekte selskapet som er oppgitt som avsender.

Foto: Gorodenkoff, Tada Images, fizkes,/Shutterstock.com

La deg ikke skremme av falske advarsler

Sprett-opp-meldinger og annonser lokker deg til å gjøre noe overilt, og de illevarslende meldingene er ofte ren svindel.

På både pc og mobiltelefon kan du få falske advarsler som hevder at pc-en eller mobilen er infisert med virus eller løsepengevirus. Meldingene ser ekte ut og er ofte utstyrt med en velkjent logo som øker troverdigheten, og hensikten er selvfølgelig å få deg til å klikke eller trykke på en farlig kobling eller betale for påstått hjelp som du virkelig ikke trenger.

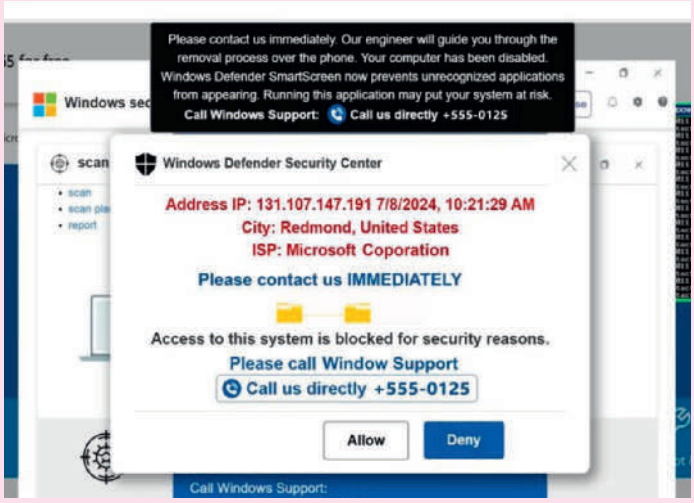
På pc-en vises ofte disse falske meldingene på bestemte hjemmesider eller som skadelige nettlesertillegg, men i noen tilfeller kan det også være snakk om bannerreklame som er designet slik at den ligner et systemvarsel i Windows eller et sikkerhetsprogram. På mobilen er det nesten alltid snakk om meldinger fra tvilsomme apper du selv har installert, eller nettleservinduer som er åpne i bakgrunnen på telefonen.

Ifølge det europeiske politisamarbeidet Europol har det skjedd en økning i bruken av skremmeprogrammer ("scareware"), som utnytter folks frykt for tap av data eller penger. Særlig eldre er utsatt. Hvis du får en slik alarmistisk melding, bør du derfor øyeblikkelig lukke vinduet uten å klikke på noe, og sørge for å ha et oppdatert antivirusprogram på datamaskinen og eventuelt også en effektiv sikkerhetsapp på mobilen. Da unngår du å bli lurt.

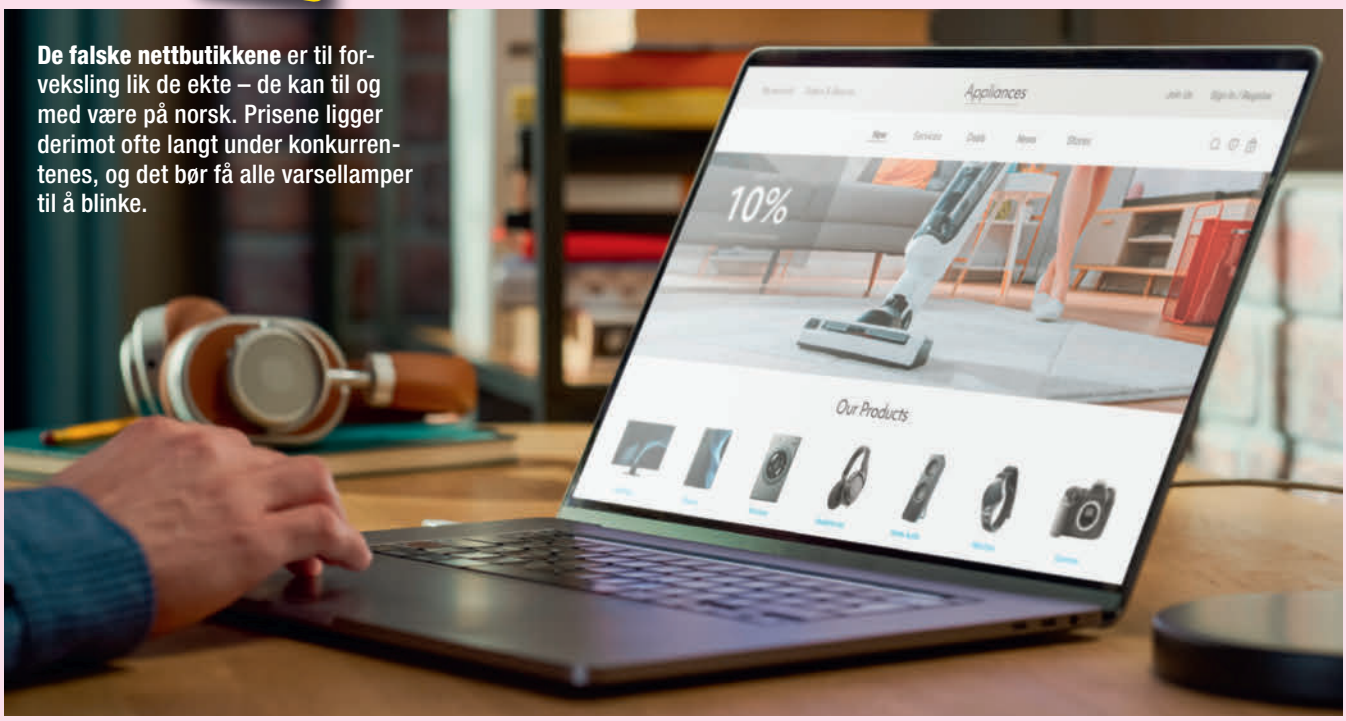
Du kan oppleve å få illevarslende meldinger om virus og andre trusler på både pc og mobil. Slike meldinger er som regel falske, så det er viktig at du holder hodet kaldt og lar være å klikke eller trykke på dem.

HVORDAN SIKRE SEG

Fordi advarslene på skjermen er falske, gjør de heller ingen skade på mobil eller pc. Skaden skjer først hvis du følger instruksene i meldingen og klikker på koblinger eller knapper i den. Det vil nemlig ofte ta deg til falske nettsider som forsøker å sanke informasjon eller hard valuta. Derfor må du sørge for å lukke de irriterende vinduene, slik at du ikke kommer til å klikke på dem ved et uhell.



Her hevder den falske advarselen å stamme fra Windows' sikkerhetsprogram Defender. I virkeligheten er det bare et åpnet nettleservindu med en falsk melding. Du kan trygt lukke vinduet ved å klikke på krysset øverst til høyre eller trykke på Alt + F4 på tastaturet.



De falske nettbutikkene er til forveksling lik de ekte – de kan til og med være på norsk. Prisene ligger derimot ofte langt under konkurrentenes, og det bør få alle varsellamper til å blinke.

Faren ved falske nettbutikker

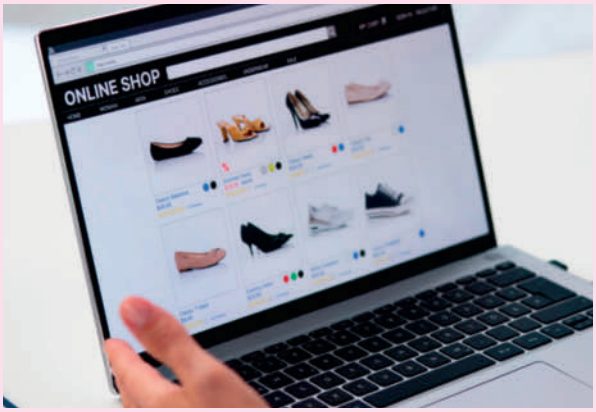
Handler du på nett, bør du være særlig på vakt hvis du besøker en nettbutikk du ikke har handlet fra tidligere – ellers risikerer du å tape både penger og data.

De senere årene har det vært en økning i antall falske nettbutikker. Derfor er det dessverre ikke usannsynlig at også du på et eller annet tidspunkt vil havne i klørne på ikke bare useriøse, men kriminelle selgere. Den sørgelige trenden har fått god hjelp av kunstig intelligens som gjør det lettere enn noensinne å lage troverdige og godt designede butikkfasader på nettet. De falske nettbutikkene kan se helt ekte ut, komplett med flotte bilder og beskrivelser som også er på norsk. Du kan til og med være så uheldig at de dukker opp blant de sponsede butikkene i et Google-søk. Bak fasaden finnes det imidlertid svindlere som kun er ute etter pengene dine. Enten sender de ikke varene i det hele tatt, eller de sender varer av dårlig kvalitet. Folkene bak kan også stjele betalingsinformasjonen og bruke den til svindel.

De falske nettbutikkene dukker ofte opp med populære tilbud eller merkevarer til usannsynlig lave priser. Hvis prisen virker for god til å være sann, er den nok også det. Da bør du være spesielt forsiktig og gå nettbutikken grundig etter i sømmene. Du kan blant annet sjekke kontaktinformasjonen

HVORDAN SIKRE SEG

Den beste og mest effektive beskyttelsen mot de falske nettbutikkene er din egen oppmerksomhet og sunne skepsis. Svindlerne blir stadig flinkere til å få butikkene til å fremstå som ekte. Det betyr at du er nødt til å følge utviklingen og være enda mer på vakt når du ser et godt tilbud eller se merkevarer til langt under normal pris. På komputer.no/2520 finner du syv gode råd til sikker netthandel.



Det er et farevarsel hvis du finner et usannsynlig godt tilbud på en nettbutikk, og det er all grunn til å være skeptisk. Se først og fremst etter organisasjonsnummeret og slå opp i foretaksregisteret på brreg.no. I tillegg kan du sjekke nettbutikken på trustpilot.com, der du kan lese andres erfaringer.

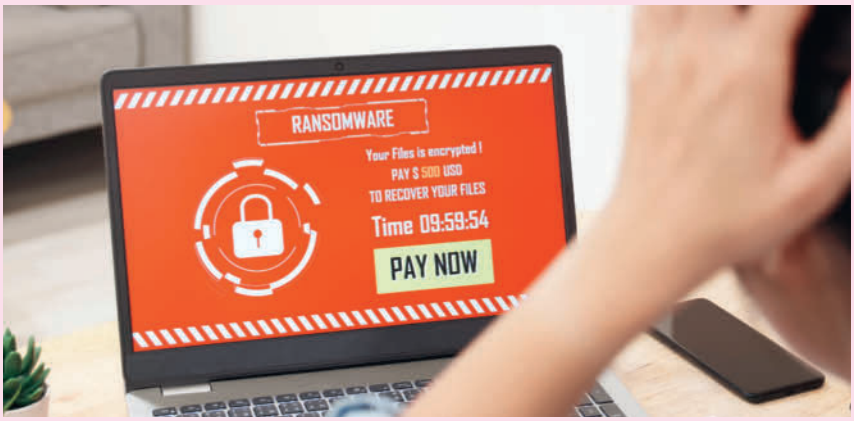
Foto: aslysun, Gorodenkoff, Andrey_Popov, Maxim Elramsisy/Shutterstock.com

for nettsiden, lese anmeldelser på **trustpilot.com** og sjekke om siden benytter en sikker tilkobling som starter med https://.

Et sikkert tegn på en falsk nettbutikk er manglende eller ufullstendig informasjon om selskapet bak. Hvis du ikke finner organisasjonsnummeret til firmaet, hvis selve hjemmesiden virker dårlig skrudd sammen eller kjøpsvilkårene er utydelige, bør du stoppe opp og revurdere tilbudet. Er du i tvil, men likevel velger å handle fra nettbutikken, er det en god idé å betale med kredittkort. Da kan du nemlig gjøre innsigelser mot kjøpet via banken, hvis det viser seg å være svindel.

Lignende sandaler var dårlige kopier

Har du blitt lurt av en falsk nettbutikk, kan du kontakte den europeiske forbrukerorganisasjonen Forbruker Europa på siden **forbrukereuropa.no**. Det gjorde Mathilde, som forteller sin historie på nettsiden. Hun forklarer hvordan hun på det som så ut til å være en lokal nettbutikk fant et par Birkenstock-sandaler til halv pris, som hun straks bestilte. Da hun senere mottok en sendingsbekreftelse, så hun imidlertid at sandalene var sendt fra Kina. Da sandalene dukket opp på hjemadressen hennes, var det dessverre også klart at det var snakk om kopivarer av dårlig kvalitet. Mathilde endte med å gjøre innsigelser overfor banken og fikk deretter pengene tilbake. Nettbutikker av denne typen, som har en annen opprinnelse enn den gir seg ut for, er blant fallgruvene du kan snuble over når du handler på nettet.



Løsepengevirus, som krypterer filer og forlanger løsepenger, er bare én blant mange typer skadevare som kan ramme mobil og pc hvis du ikke er tilstrekkelig årvåken.

Pc-en infiseres med skadevare

Hvis du er uheldig og får skadevare på pc og mobil, risikerer du både langsomme og ustabile enheter, i tillegg til tap av både penger og personlige data.

Skadevare ("malware") er programmer som kan infisere datamaskiner og mobiltelefoner. De ondsinnede programmene kan komme fra mange kilder. De kan få innpass på enhetene via farlig e-post, falske nedlastinger og infiserte nettsider.

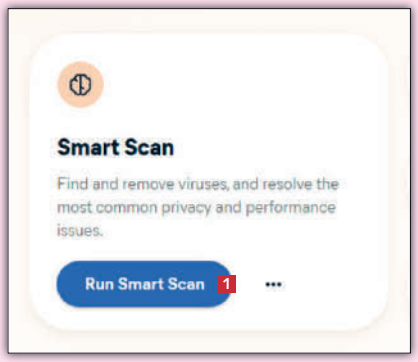
Når skadevaren rammer, kan viruset stjele personopplysninger som brukernavn, passord og betalingsinformasjon, eller den kan gjøre pc eller smarttelefon tregere og mindre stabil. Derfor gjelder det å være oppmerksom på hva du klikker på når du sjekker e-post eller besøker hjemmesider. Pass på at du utelukkende laster ned programmer fra troverdige kilder, som komputer.no.

Sørg også for at du holder både Windows og programmene oppdatert, slik at produsentene har mulighet til å tette kritiske sikkerhetshull som kan gjøre deg og enhetene dine sårbare. Det er også viktig at du har et velfungerende antivirusprogram på maskinen – for eksempel Avast One Essential, som du kan laste ned fra **komputer.no/2520**.

HVORDAN SIKRE SEG

Den viktigste beskyttelsen mot skadevare er å sørge for at den grunnleggende virusbeskyttelsen er på plass, for eksempel i form av Avast One Essential. Først deretter kan du vurdere å supplere med ytterligere programmer for å bekjempe skadevare. Prøv gjerne Malwarebytes Antimalware, som du også kan laste ned fra hjemmesiden vår.

Last ned fra **komputer.no/2520**



1 Last ned og installer Avast One Essential fra nettsiden vår. Start programmet og klikk på **Run Smart Scan** 1 for å gi maskinen en grundig virussjekk.