SociALL

TILGJENGELIGGJØRING AV DIGITALE VERKTØY I HELSE- OG OMSORGSSEKTOREN

Emne 1.3. Grunnleggende om nett- og cybersikkerhet

Finansiert av Den europeiske union. Synspunktene og meningene som kommer til uttrykk, er imidlertid kun forfatternes egne og gjenspeiler ikke nødvendigvis synspunktene til EU eller European Education and Culture Executive Agency (EACEA). Verken EU eller EACEA kan holdes ansvarlig for dem.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.

MedicalScan

åpenhet

Co-funded by the European Union

Innholdsfortegnelse

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medical car
åpenhet
Co-funded by the European Union

SociALL

Introduksjon til kurset

1. Kursoversikt
2. Målgruppe
3. Mål for opplæringen

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medicalscan
åpenhet
Co-funded by the European Union

Introduksjon til kurset

1. Oversikt over kurset

Hva handler kurset om?

Kurset "Grunnleggende om nett- og cybersikkerhet" er utviklet for å gi sosialarbeidere grunnleggende kunnskaper og ferdigheter til å **beskytte sensitiv data og ivareta nettsikkerhet** i jobbsammenheng. Ved å studere dette heftet, vil lesere lære hvordan man kan **identifisere** og **redusere** vanlige cyber-sikkerhetsrisikoer, og få tips til forebyggende tiltak som er er enkle å implementere.

Nytteverdi

Undersøkelser gjort iSociALL-prosjektet viste behov for økt kunnskap om nett- og cybersikkerhet i omsorgssektoren. Cybersikkerhet er et spesielt **viktig og aktuelt** tema i en periode med økt risiko og bekymringer for personvern i forbindelse med helse- og personopplysninger. Flere cyberangrep mot **sårbare** organisasjoner, som for eksempel den senere tids mange tilfeller av løsepengevirus mot europeiske sykehus, krever økt oppmerksomhet og kunnskap.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medicalscan
åpenhet
Co-funded by the European Union

Introduksjon til kurset

2. Målgruppe

Hvem er kurset for?

Alle **som jobber i omsorgssektoren** kan ta dette kurset, da alle bruker digitale verktøy daglig og dermed er utsatt for nettrisiko. Kurset består for det meste av forklaringer, tips og beste praksis som for de fleste kan anvendes individuelt og uten store tekniske ferdigheter. Det meste av innholdet kan brukes i yrkeslivet, men mye kan også brukes i forbindelse med personlig bruk av digitale verktøy.

Passer det for meg?

Kurset er tilpasset **alle arbeidstakere** og gir en enkel og nyttig innføring og veiledning i nettsikkerhet og nettvett. Alle som er vant til å bruke digitale verktøy i yrkeslivet, har forutsetninger for å forstå innholdet i dette heftet.

Co-funded by the European Union

Introduksjon til kurset

3. Mål for opplæringen

Hva kan jeg lære av kurset?

- Forstå **viktigheten** av cybersikkerhet og sikkerhet på nettet.
- Forstå **risikoene** og de vanligste **truslene**
- Forstå den **menneskelige faktoren** i cyberangrep
- Lære om **tiltak** for databeskyttelse og sikkerhet på nettet som er **enkle å implementere**
- Utnytte nyttige **ressurser**, **verktøy** og globalt akseptert **beste praksis** for å øke sikkerheten.

Hva vil det endre?

Etter endt opplæring vil deltakerne og deres organisasjon være i stand til å bedre:

- **Integrere** nettsikkerhet i virksomheten
- **Identifisere** og **håndtere cybersikkerhetsrisikoer**
- **Endre vaner** som gjør dem **sårbare**
- **Gi opplæring og råd til** kolleger for å skape en **tryggere organisasjon.**
- **Videreformidle** kunnskapen til **sårbare brukere**

Co-funded by the European Union

SociALL

1. Grunnleggende om cybersikkerhet og sikkerhet på nettet

1. Viktigheten av cybersikkerhet og sikkerhet på nettet
2. Helsearbeidernes ansvar for pasientenes dataintegritet
3. Menneskelige feil og uaktsomhet er den viktigste innfallsporten til nettkriminalitet.
4. Hva kan vi gjøre? Identifisere og behandle menneskelige sårbarheter

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
MPWA
Medical Car
åpenhet
Co-funded by the European Union

1. Grunnleggende om cybersikkerhet og sikkerhet på nettet

1.1. Betydningen av cybersikkerhet og sikkerhet på nettet

Cybersikkerhet er ikke bare et moteord

Det er et skjold som beskytter oss mot ulike risikoer på nettet, inkludert identitetstyveri, økonomisk svindel, tyveri av personopplysninger og nettangrep.

Cybersikkerhet er en trippel beskyttelse

I pleie- og omsorgssektoren har cybersikkerhet som oppgave å beskytte den enkelte ansatte, organisasjonen og pasienter/brukere.

Cyberangrep er den nye kriminaliteten

Som den nylige bølgen av løsepengevirusangrep mot pleieinstitusjoner (sykehus, aldershjem osv.) har vist, blir nettangrep stadig farligere og mer truende i pleie- og omsorgssektoren.

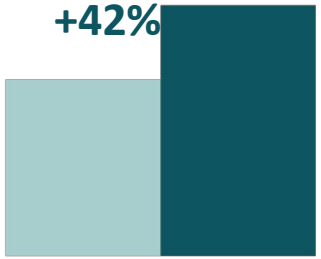
Konklusjon: **Faren** for nettkriminalitet har aldri vært så reell som nå. Vår **avhengighet** av digitale verktøy i alle aspekter av livet gjør oss til **sårbare** mål, så lenge vi ikke gjør noe **for** å ivareta vår digitale sikkerhet.

Co-funded by the European Union

1. Grunnleggende om cybersikkerhet og sikkerhet på nettet

1.1. Betydningen av cybersikkerhet og sikkerhet på nettet

Noen få tall fra "Cyber Attack Trends: 2022 Mid-Year Report" viser at faren er reell. Bare i 2022 har:



Cyberangrep mot helseinstitusjoner økte med **42 %** sammenlignet med forrige periode.

Datainnbrudd i helsesektoren hatt en gjennomsnittlig totalkostnad på **10,10 millioner amerikanske dollar** per hendelse.

Helseorganisasjoner opplevde **1426** (dokumenterte) **angrep per uke** over hele verden.

1 av 42 helseorganisasjoner blitt utsatt for et løsepengevirusangrep i tredje kvartal av 2022.

Konklusjon: **Faren** for nettkriminalitet har aldri vært så reell som nå. Vår **avhengighet** av digitale verktøy i alle aspekter av livet gjør oss til **sårbare** mål, så lenge vi ikke gjør noe **for** å ivareta vår digitale sikkerhet.

Co-funded by the European Union

1. Grunnleggende om cybersikkerhet og sikkerhet på nettet

1.2. Helsearbeidernes ansvar for pasientenes dataintegritet

Tillit er grunnlaget og fundamentet i forholdet mellom pleier og pasient. En sentral del av denne tilliten er evnen til å håndtere og beskytte pasientenes sensitive og personlige opplysninger på en ansvarlig måte.

Pasientdata er en skattekiste av **personlig** og ofte **sensitiv** informasjon.

- Medisinsk historie
- Behandlingsplaner
- Livshygiene
- Kontaktinformasjon
- Personnummer

Helse- og omsorgspersonell sitter på store mengder **person-** og helseopplysninger som kan være av interesse for en **rekke ulike aktører**, fra selskaper som selger produkter til svindlere eller andre personer med onde hensikter på jakt etter enkle ofre.

Viktigere er det at disse dataene, uansett verdi, er **personlige** og **private**. Helsepersonell har et stort ansvar for å beskytte dem, og det er de forpliktet til overfor pasientene som betror dem dataene sine.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medicalscan
åpenhet
Co-funded by the European Union

1. Grunnleggende om cybersikkerhet og sikkerhet på nettet

1.2. Helsearbeidernes ansvar for pasientenes dataintegritet

Selv om digital behandling av pasientdata har gjort livet enklere og mer effektivt for pleiepersonalet, representerer det en **sårbarhet** og et **nytt område som må beskyttes**.

Hva med GDPR? HIPAA?

Det finnes juridiske forpliktelser som skal sikre et minimum av beskyttelse. Pleiepersonalet bør imidlertid ikke iverksette personverntiltak bare for å overholde disse forpliktelsene: Det er deres **etiske plikt** å ivareta pasientenes **verdighet** og **personvern.**

Personvern er mer enn bare overholdelse av juridiske forpliktelser.

Pleiepersonalet må innse hvilke **konsekvenser datainnbrudd** kan få, og forstå hvor stort **og viktig ansvaret** deres er. Pasientenes tillit er avhengig av denne erkjennelsen, og det samme er helsearbeidernes moralske forpliktelse til å beskytte pasientene.

Co-funded by the European Union

1. Grunnleggende om cybersikkerhet og sikkerhet på nettet

1.3. Menneskelige feil og uaktsomhet; den viktigste årsaken til nettkriminalitet.

Menneskelige feil og uaktsomhet er det nettkriminelle utnytter. Det er den enkleste **innfallsporten,** og kan sammenlignes med å la døren stå på vidt gap uten tilsyn når man forlater en pleieinstitusjon om natten.

Det er mulig å hacke programvare og databaser ved å utnytte **tekniske sårbarheter**, men det er svært sjeldent og utgjør bare en liten del av alle cyberangrep. I de aller fleste tilfeller går nettkriminelle rett og slett gjennom **dører som** mennesker har **etterlatt åpne** - enten på grunn av feil eller uaktsomhet - for å skaffe seg **uautorisert tilgang** og **kompromittere sensitiv informasjon**.

"Jeg er en omsorgsarbeider, ikke en IT-ekspert. Hvorfor skal jeg bruke tid på dette?"

I nesten alle nettangrep som pleie- og omsorgssektoren har vært vitne til i det siste (phishing, løsepengevirus osv.), har årsaken til innbruddet ikke vært et defekt antivirusprogram, svak programvare eller en suboptimal teknisk arkitektur: Disse angrepene utnytter nesten alltid **menneskelige feil**, ofte fra helsepersonalet selv.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
MPWA
Medicalscan
åpenhet
Co-funded by the European Union

1. Grunnleggende om cybersikkerhet og sikkerhet på nettet

1.4. Hva kan vi gjøre? Identifisere og behandle menneskelige sårbarheter

Cybersikkerhet i pleie- og omsorgssektoren handler ikke bare om enkeltpersoners innsats - hvis én gjør en feil, påvirker det alle de andre. Det handler om **kollektivt ansvar**, **bevissthet**, implementering av **beste praksis** og **opplæring**.

Cybersikkerhet er et institusjonelt komplekst tema, ettersom feil begått av én påvirker alle (som eksemplifisert med løsepengevirusene mange sykehus ble ofre for). Derfor handler cybersikkerhet om å **forbedre det kollektive forsvaret** mot cybertrusler, og ikke bare om å forbedre den enkeltes atferd.

Det innebærer en **kollektiv innsats** for å **øke bevisstheten, øke ansvaret og eierskapet, utdanne de ansatte** om cybertrusler, innføre og bruke prosesser som integrerer **beste praksis,** osv.

På **individnivå innebærer** cybersikkerhet ikke bare om **respekt for protokoller** og prosesser, men også om en forståelse av sin egen posisjon som **aktør i institusjonens cybersikkerhet,** noe som innebærer **kritisk tenkning og bevisstgjøring** om farer, bidrag til **opplæring eller veiledning** og **aktivt engasjement og** eierskap.

Co-funded by the European Union

1. Grunnleggende om cybersikkerhet og sikkerhet på nettet

1.4. Hva kan vi gjøre? Identifisere og behandle menneskelige sårbarheter

Cybersikkerhet er en usikker vitenskap: Innbrudd skjer fortsatt i godt beskyttede og velutdannede strukturer. Organisasjoner bør ikke forsømme å iverksette **korrigerende tiltak og beredskap** i tilfelle brudd.

Selv med en forbedret tilnærming til cybersikkerhet, bedre prosesser, bedre utdannet personale osv. kan datainnbrudd og cyberangrep fortsatt forekomme, likevel i betydelig mindre grad. Det finnes ingen tiltak som gir 100 % beskyttelse, og det er derfor avgjørende for omsorgsinstitusjoner å ha komplette strategier på plass som kan iverksettes umiddelbart i tilfelle brudd, og å være forberedt på krisehåndtering, mottiltak, gjenoppretting av kontroll og konsekvensreduksjon.

Disse strategiene skal imidlertid utvikles av de **tekniske teamene,** og innebærer et mer **spesifikt, teknisk innhold**. Korrigerende tiltak og beredskap er derfor ikke en del av dette pensumet, selv om det er helt nødvendig for enhver omsorgsorganisasjon.

Co-funded by the European Union

2. Oversikt over de vanligste truslene

1. Beskyttelse av pasienter
2. Phishing-angrep
3. Ondsinnet programvare
4. Sosial manipulering

Co-funded by the European Union

2. Oversikt over de vanligste truslene

2.1. Beskyttelse av pasienter

Trusler på nettet kan ramme og skade

Individuelle ansatte

Omsorgs-orga nisasjoner

Pasienter

Dette gjelder særlig visse pasientgrupper som er mer **utsatt for** å bli ofre for nettangrep, for eksempel **isolerte eldre mennesker.**

Pleiepersonalet kan beskytte pasientene sine når de oppdager en sikkerhetsrisiko på nettet ved å gjøre følgende

Observere deres atferd på nettet

Diskutere med dem og spørre om deres liv på nettet

Identifisere potensielle risikoer i deres atferd på nettet

Advare dem om farer som er identifisert

Opplyse dem om sikkerhet på nettet

Co-funded by the European Union

2. Oversikt over de vanligste truslene

2.2. Phishing-angrep

Phishing-angrep er **umoralske** forsøk på å få tak i **sensitiv informasjon** ved å utgi seg for å være **pålitelige** aktører. I pleie- og omsorgssektoren er det flere ulike former for phishing-angrep:

Svindel med kompromittering av e-post fra bedrifter ("Whaling")

Sofistikerte angrep som forsøker å **lure** ansatte til å overføre penger eller avsløre sensitiv informasjon.

Disse svindelforsøkene sendes ofte via **e-post** til økonomi- eller regnskapsavdelinger ved å **utgi seg for å være** høytstående ledere eller autorisert personell.

Disse phishing-e-postene ber vanligvis om hastebetalinger, endringer i leverandøropplysninger eller sensitiv informasjon om ansatte, og spiller på det **hierarkiske forholdet** mellom avsender og mottaker.

From: CEO@acmecorp.com
To: Jane@acmecorp.com
Subject: Urgent

I need you to initiate a wire transfer in the sum of $45,250 to the account below. I am boarding a flight and this needs to be done right now. Can you please get this done? Send confirmation of the transfer immediately.

Thanks

Kilde: Proofpoint

CLUES

- ✔ Avsender bruker høyere hierarkisk posisjon
- ✔ Følelsen av at det haster - ingen tid til å sjekke/protestere
- ✔ Avsender kan ikke snakke i telefonen, bare skrive
- ✔ Forfalsket domenenavn på avsenderens e-postadresse

Co-funded by the European Union

2. Oversikt over de vanligste truslene

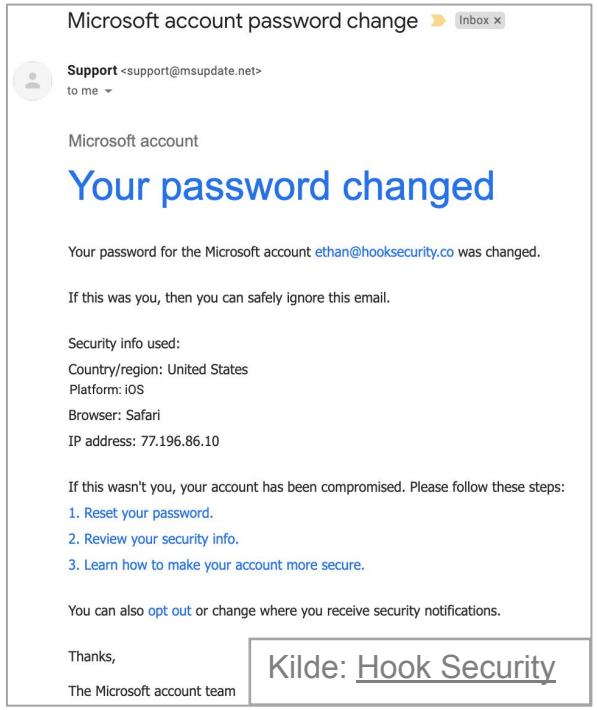
2.2. Phishing-angrep

Phishing-angrep er **umoralske** forsøk på å få tak i **sensitiv informasjon** ved å utgi seg for å være **pålitelige** enheter. I pleie- og omsorgssektoren er det flere ulike former for phishing-angrep:

Phishing-angrep med innhenting av legitimasjon

Phishing-angrep går ut på å **stjele** brukernavn, passord og annen **påloggingsinformasjon** for å skaffe seg **uautorisert tilgang** til omsorgssystemer. Disse svindelforsøkene bruker ofte overbevisende **kopier** av legitime påloggingssider, for eksempel EMR-portaler eller intranett.

Angriperne sender phishing-e-poster eller omdirigerer ofrene til **ondsinnede nettsteder** der de oppgir påloggingsinformasjonen sin, **uvitende** om at kriminelle får tilgang til organisasjonens sensitive data.



Microsoft account password change Inbox ×

Support <support@msupdate.net>
to me

Microsoft account

Your password changed

Your password for the Microsoft account ethan@hooksecurity.co was changed.

If this was you, then you can safely ignore this email.

Security info used:
Country/region: United States
Platform: iOS
Browser: Safari
IP address: 77.196.86.10

If this wasn't you, your account has been compromised. Please follow these steps:
1. Reset your password.
2. Review your security info.
3. Learn how to make your account more secure.

You can also opt out or change where you receive security notifications.

Thanks,
The Microsoft account team

Kilde: Hook Security

CLUES

- ✔ Forfalsket domenenavn på avsenderens e-post (f.eks. @msupdate.net)
- ✔ Et annet design på e-posten enn de vanlige e-postene fra selskapet
- ✔ Forespørsel om å reagere på noe du ikke har gjort (f.eks. levere en pakke du ikke har bestilt)

Co-funded by the European Union

2. Oversikt over de vanligste truslene

2.2. Phishing-angrep

Phishing-angrep er **umoralske** forsøk på å få tak i **sensitiv informasjon** ved å utgi seg for å være **pålitelige** enheter. I pleie- og omsorgssektoren er det flere ulike former for phishing-angrep:

Phishing-e-poster med skadelig programvare

Phishing-e-poster med skadelig **programvare** er utformet for å **lure** mottakerne til å laste ned og kjøre **skadelig programvare**. Disse e-postene inneholder ofte **infiserte vedlegg** eller **lenker** til kompromitterte nettsteder.

Organisasjoner i **helsevesenet** er **spesielt utsatt** for skadevareangrep, ettersom vellykkede innbrudd kan kompromittere pasientjournaler, forstyrre driften eller til og med sette liv i fare.

Kilde: Imperva

CLUES

- ✔ Stavefeil, grammatiske feil og tegnsettingsfeil
- ✔ Lenker i e-postens brødtekst som omdirigerer til uventede nettsteder (hold musepekeren over lenken for å se URL-adressen)
- ✔ Trussel (f.eks. sperret konto) eller følelse av hastverk
- ✔ Vedlegg som du ikke har bedt om/utløst
- ✔ Uvanlig forespørsel, tone eller hilsen

Co-funded by the European Union

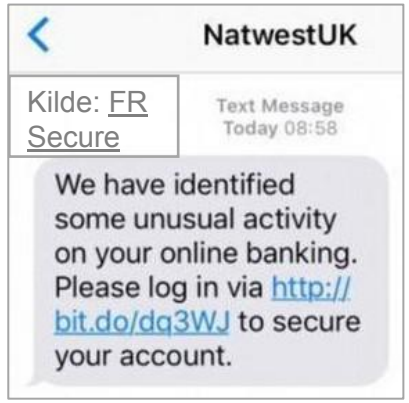
2. Oversikt over de vanligste truslene

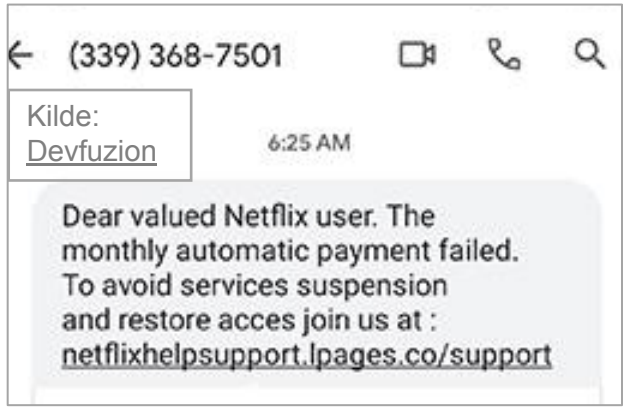
2.2. Phishing-angrep

Phishing-angrep er **umoralske** forsøk på å **få tak i sensitiv informasjon** ved å utgi seg for å være **pålitelige** enheter. I pleie- og omsorgssektoren er det flere ulike former for phishing-angrep:

Vishing- og smishing-angrep

Vishing (via talemeldinger eller telefonsamtaler) og **smishing** (via SMS) kan være hvilket som helst av de tidligere phishing-angrepene. De erstatter ganske enkelt den tradisjonelle e-posten med et annet kommunikasjonsmiddel (SMS, telefonsamtale osv.).





CLUES

Vishing

- ✔ Krevende tone: svindlere utnytter frykt eller panikk
- ✔ Forespørsel om konfidensiell eller personlig informasjon
- ✔ De fleste av organisasjonene svindlerne utgir seg for å representere ringer ikke til kunder direkte.

Smishing

- ✔ Ukjent nummer, ikke referert til på Internett
- ✔ Besøk nettsiden til den falske avsenderen - f.eks. skriver bankene på nettsidene sine at de ikke sender SMS.
- ✔ Ta direkte kontakt med selskapets kundeservice

Co-funded by the European Union

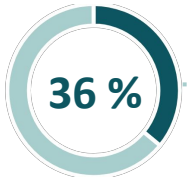
2. Oversikt over de vanligste truslene

2.2. Phishing-angrep

Phishing-angrep er **umoralske** forsøk på å **få tak i sensitiv informasjon** ved å utgi seg for å være **pålitelige** enheter. Noen tall fra **2022** viser hvor utbredt, sofistikert og farlig phishing faktisk er (Kilde: Stationx.net).

3.4 MRD

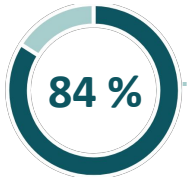
Phishing er den **vanligste formen for nettkriminalitet**. Anslagsvis **3,4 milliarder e-poster per dag** er phishing-angrep fra nettkriminelle. Det er over en **billion** phishing-e-poster i **året**.



36 % av alle datainnbrudd involverer phishing.

Det anslås at **etterligning av e-post** står for **1,2 % av all e-posttrafikk** globalt.

1.2 %



84 % av alle organisasjoner ble utsatt for minst **ett phishing-forsøk** i 2022.

Den gjennomsnittlige klikkefrekvensen for en phishing-kampanje er **17,8 %.**

3 %

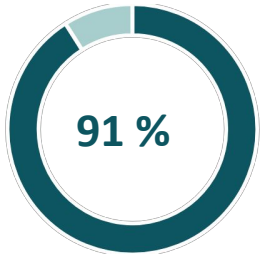
I gjennomsnitt klikker 3 % av de ansatte på en ondsinnet lenke i en phishing-e-post.

Co-funded by the European Union

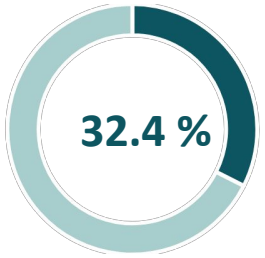
2. Oversikt over de vanligste truslene

2.2. Phishing-angrep

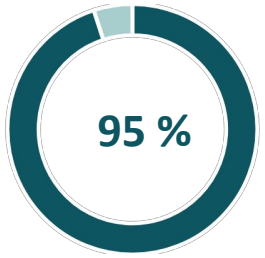
Phishing-angrep er **umoralske** forsøk på å **få tak i sensitiv informasjon** ved å utgi seg for å være **pålitelige** enheter. Noen tall fra **2022** viser hvor utbredt, sofistikert og farlig phishing faktisk er (Kilde: Stationx.net).



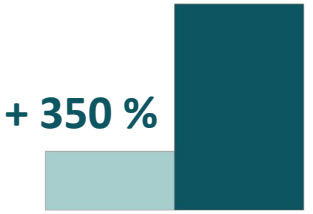
av alle nettangrep begynner med en **phishing-e-post.**



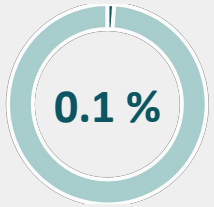
av **uopplærte** ansatte kan falle for phishing-svindel



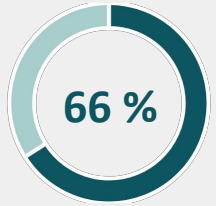
av vellykkede sikkerhetsbrudd er direkte forårsaket av **menneskelige feil.**



Små organisasjoner har **350 %** større sannsynlighet for å bli **utsatt** for **phishing** enn større organisasjoner.



0,1 % av alle e-postbaserte phishing-angrep er ansvarlige for **66 %** av alle sikkerhetsbrudd. (*vanligvis målrettede, personaliserte "spear-phishing"-angrep*)



Co-funded by the European Union

2. Oversikt over de vanligste truslene

2.3. Ondsinnet programvare

Malwares er et paraplybegrep som omfatter ulike typer ondsinnet programvare som er utviklet for å forstyrre, skade eller få tilgang til datasystemer, nettverk eller enheter. I omsorgssektoren forekommer malwares for det meste i form av:

Virus

Virus er ondsinnede programmer som **infiserer** filer eller programvarer på en datamaskin og kopierer seg selv når de infiserte filene **kjøres**. De kan forårsake skade på data, programvare og maskinvarekomponenter.

For eksempel kan phishing-e-post eller SMS med skadelig programvare lure brukere til å klikke på **lenker** eller laste ned **filer** som er infisert. Disse infiserte filene eller koblingene "aktiveres" først når brukeren klikker på dem, og det er derfor viktig å være forsiktig når man mottar uønskede e-poster.

FORSIKTIG

Mange svindlere utnytter **frykten for virus** til å infisere deg: Hvis en popup-melding fra et antivirusprogram du ikke har, signaliserer en potensiell infeksjon på datamaskinen din og tilbyr deg å løse problemet ved å klikke på en knapp eller ringe et nummer, bør du ikke reagere, for det kan godt hende at du blir infisert.

Kilde: Microsoft-Community

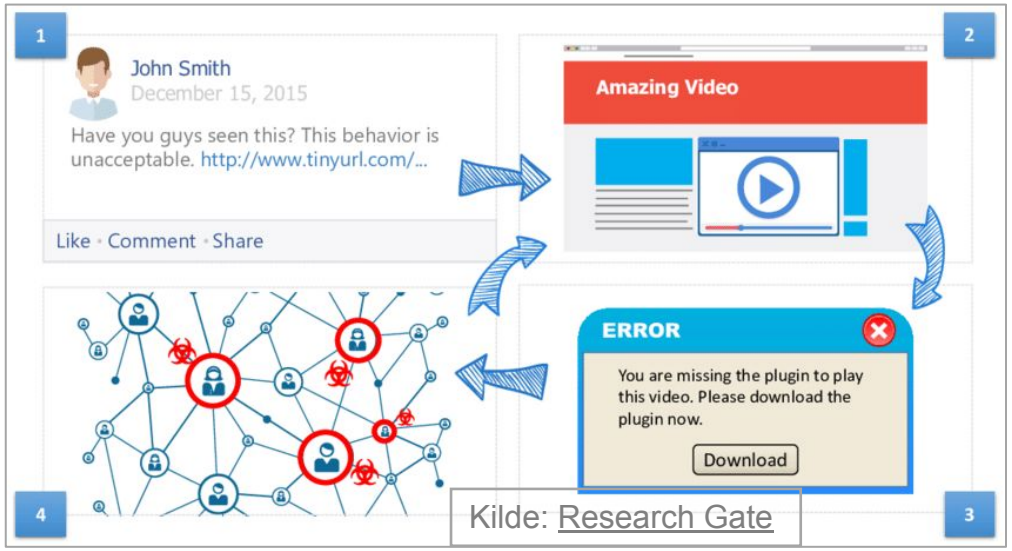
2. Oversikt over de vanligste truslene

2.3. Ondsinnet programvare

Malwares er et paraplybegrep som omfatter ulike typer ondsinnet programvare som er utviklet for å forstyrre, skade eller få tilgang til datasystemer, nettverk eller enheter. I omsorgssektoren forekommer malwares for det meste i form av:

Trojanere

Trojanere, eller trojanske hester, er malware **forkledd som legitim programvare**. De lurer brukere til å installere dem, ofte ved å fremstå som harmløse filer eller programmer. Når trojanere er installert, kan de utføre ulike ondsinnede aktiviteter, som å stjele sensitive data, endre informasjon eller gi uautorisert tilgang til angripere. Trojanere utløses ofte av phising-e-poster eller -meldinger.



Kilde: Research Gate

CLUES

- ✔ Datamaskinen kjører saktere enn vanlig.
- ✔ Uautoriserte apper vises på enheten.
- ✔ Hyppige krasj og frysing av enheten.
- ✔ Hyppige popup-vinduer.
- ✔ Noen programmer starter ikke.
- ✔ Hyppige avbrudd i internettforbindelsen.

Co-funded by the European Union

2. Oversikt over de vanligste truslene

2.3. Ondsinnet programvare

Malwares er et paraplybegrep som omfatter ulike typer ondsinnet programvare som er utviklet for å forstyrre, skade eller få tilgang til datasystemer, nettverk eller enheter. I omsorgssektoren forekommer malwares for det meste i form av:

Ransomwares

Løsepengevirus er en type skadevare som krypterer filer på offerets datamaskin eller enhet og gjør dem **utilgjengelige inntil løsepenger er betalt**. Løsepengeangrep krever vanligvis betaling i kryptovaluta og kan føre til store økonomiske tap og tap av data.

Sykehus og helseinstitusjoner, hvis systemer er avgjørende for driften, er spesielt utsatt. I 2022 var **66 %** av alle sykehusene i USA målet (ikke alltid offeret) for et løsepengevirusangrep. I rundt **61 %** av tilfellene av løsepengevirus hos organisasjoner i helsesektoren i 2022 ble det betalt løsepenger.

Kilde: Healthcare IT News

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medicalcar
åpenhet
Co-funded by the European Union

2. Oversikt over de vanligste truslene

2.3. Ondsinnet programvare

Malwares er et paraplybegrep som omfatter ulike typer ondsinnet programvare som er utviklet for å forstyrre, skade eller få tilgang til datasystemer, nettverk eller enheter. I omsorgssektoren forekommer malwares for det meste i form av:

Dataormer

Dataormer er frittstående skadevareprogrammer som **replikerer** seg selv på tvers av nettverk, vanligvis ved å utnytte sårbarheter i operativsystemer eller nettverksprotokoller.

De kan spre seg raskt og forårsake **overbelastning i nettverket** eller utføre andre ondsinnede aktiviteter.

Spionprogrammer

Spionprogrammer er utviklet for å **overvåke** og samle inn informasjon om brukerens aktiviteter på datamaskinen eller enheten i **hemmelighet.**

De kan **spore tastetrykk, ta skjermbilder, registrere surfevaner** og stjele **sensitiv informasjon** som passord og finansielle data.

Addwares

Addwares er uønsket programvare som viser **reklame**, ofte i form av popup-annonser eller nettleseromdirigeringer.

Selv om adware ikke er skadelig i seg selv kan det **svekke systemytelsen**, kompromittere **personvernet** og føre til **ytterligere infeksjoner** hvis det ikke fjernes.

Co-funded by the European Union

2. Oversikt over de vanligste truslene

2.3. Ondsinnet programvare

Malwares er et paraplybegrep som omfatter ulike typer ondsinnet programvare som er utviklet for å forstyrre, skade eller få tilgang til datasystemer, nettverk eller enheter. I omsorgssektoren forekommer malwares for det meste i form av:

Keyloggere

Keyloggere er en type spionprogramvare som registrerer **tastetrykk** fra en bruker og samler inn sensitiv informasjon som **passord**, **brukernavn** og kredittkortopplysninger.

Angripere kan bruke keyloggere til å stjele personopplysninger og begå identitetstyveri.

Botnett

Botnett er **nettverk av kompromitterte datamaskiner** eller enheter som kontrolleres av angripere.

Botnett kan brukes til å utføre distribuerte tjenestenektangrep (DDoS-angrep), sende **søppelpost** eller utføre andre ondsinnede aktiviteter **uten at eierne er klar over det**.

Bakdører

Bakdører er **skjulte inngangspunkter** eller sårbarheter som angripere bevisst har skapt i programvare eller systemer, og som gir **uautorisert tilgang for fremtidig utnyttelse eller kontroll**.

Disse bakdørene gjør det mulig for angripere å ta kontroll over enheten i **hemmelighet**, installere annen skadelig programvare, registrere tastetrykk osv.

Co-funded by the European Union

2. Oversikt over de vanligste truslene

2.3. Ondsinnet programvare

Disse ulike typene malware er ofte kombinert i ett program eller én fil. Noen tall fra **2022** viser hvor utbredt, sofistikert og farlig malwares er (Kilde: Getastra.com).

1 milliard

560 000 nye skadeprogrammer oppdages **daglig**. Det finnes i dag over **1 milliard** skadevareprogrammer.

$4.54 M

Hvert minutt blir **fire selskaper utsatt** for løsepengevirusangrep. **Pleie- og omsorgssektoren** er den sektoren som er mest utsatt, og som betaler mest løsepenger. Gjennomsnittskostnaden for et løsepengevirusangrep er **4,54 millioner dollar.**

50%

Bare **50 %** av organisasjonene som betalte **løsepenger,** klarte å **gjenopprette dataene sine**. **64 %** av organisasjonene som ble utsatt for løsepengevirusangrep, ble **infisert**.

+87%

I løpet av det siste tiåret har antallet infeksjoner med skadevare **økt med 87 %. Trojanere står** for **58 %** av all skadevare på datamaskiner. Kostnadene ved nettkriminalitet forventes å nå **8 billioner dollar i 2023**.

Co-funded by the European Union

2. Oversikt over de vanligste truslene

2.4. Sosial manipulering

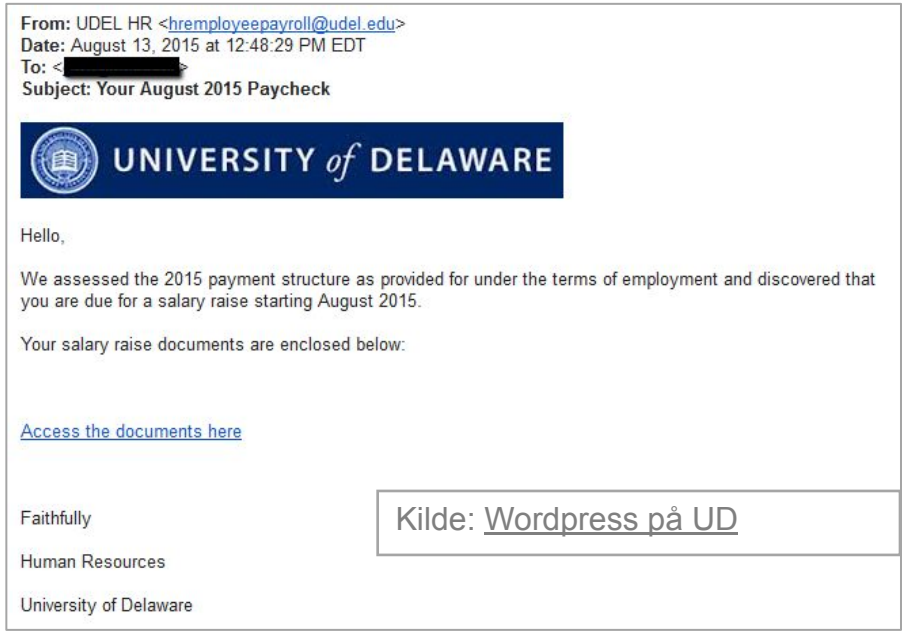
Med sosial manipulering menes bruk av sosiale taktikker for å utnytte ansattes tillit, uaktsomhet eller uvitenhet for å få tak i konfidensiell informasjon. Selv om phishing- og skadevareangrep ofte utnytter disse sårbarhetene og **overlapper** med sosial manipulering, bruker ren sosial manipulering mer direkte sosiale **taktikker,** og kan omfatte følgende:

Spear phishing

Spear phishing er en **målrettet form for phishing** som **skreddersyr angrepet** til bestemte personer eller organisasjoner.

Angriperne samler inn informasjon om målene sine fra sosiale medier, offentlige databaser eller tidligere interaksjoner for å tilpasse phishing-e-postene og øke sannsynligheten for å lykkes.

Spear phishing-meldinger kan inneholde ulike typer skadevare, direkte be om personopplysninger (f.eks. telefonnummer for å løse en "hastesak"), be om betaling av fakturaer osv.



From: UDEL HR <hremployeepayroll@udel.edu>
Date: August 13, 2015 at 12:48:29 PM EDT
To: <[redacted]>
Subject: Your August 2015 Paycheck

UNIVERSITY of DELAWARE

Hello,

We assessed the 2015 payment structure as provided for under the terms of employment and discovered that you are due for a salary raise starting August 2015.

Your salary raise documents are enclosed below:

Access the documents here

Faithfully

Human Resources

University of Delaware

Kilde: Wordpress på UD

2. Oversikt over de vanligste truslene

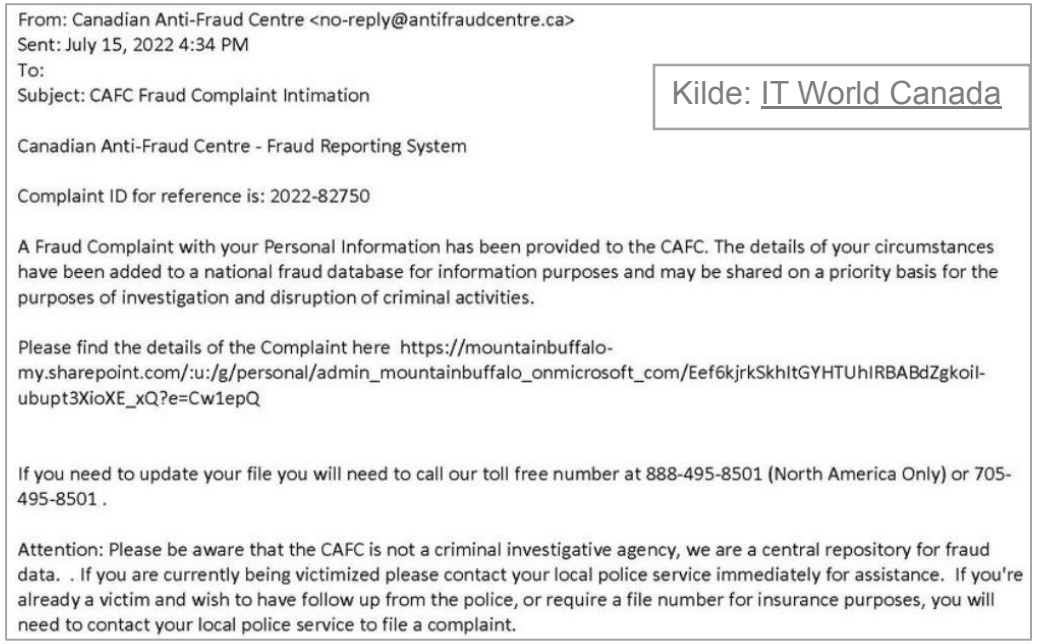
2.4. Sosial manipulering

Med sosial manipulering menes bruk av sosiale taktikker for å utnytte ansattes tillit, uaktsomhet eller uvitenhet for å få tak i konfidensiell informasjon. Selv om phishing- og skadevareangrep ofte utnytter disse sårbarhetene og **overlapper** med sosial manipulering, bruker ren sosial manipulering mer direkte sosiale **taktikker,** og kan omfatte følgende:

Pretexting

Pretexting innebærer å skape et oppdiktet **scenario eller påskudd** for å manipulere personer til å avsløre konfidensiell informasjon eller utføre bestemte handlinger.

Angriperne utgir seg ofte for å være **betrodde personer**, for eksempel IT-støttepersonell, politifolk eller bedriftsledere, for å vinne målpersonens tillit og få tak i sensitiv informasjon. Pretexting-svindel kan ha svært liknende utfall som phishing-svindel, med krav om betaling, stjeling av legitimasjon eller personopplysninger osv.



From: Canadian Anti-Fraud Centre <no-reply@antifraudcentre.ca>
Sent: July 15, 2022 4:34 PM
To:
Subject: CAFC Fraud Complaint Intimation

Kilde: IT World Canada

Canadian Anti-Fraud Centre - Fraud Reporting System

Complaint ID for reference is: 2022-82750

A Fraud Complaint with your Personal Information has been provided to the CAFC. The details of your circumstances have been added to a national fraud database for information purposes and may be shared on a priority basis for the purposes of investigation and disruption of criminal activities.

Please find the details of the Complaint here https://mountainbuffalo-my.sharepoint.com/:u:/g/personal/admin_mountainbuffalo_onmicrosoft_com/Eef6kjrkSkhItGYHTUhIRBABdZgkoil-ubupt3XioXE_xQ?e=Cw1epQ

If you need to update your file you will need to call our toll free number at 888-495-8501 (North America Only) or 705-495-8501 .

Attention: Please be aware that the CAFC is not a criminal investigative agency, we are a central repository for fraud data. . If you are currently being victimized please contact your local police service immediately for assistance. If you're already a victim and wish to have follow up from the police, or require a file number for insurance purposes, you will need to contact your local police service to file a complaint.

Co-funded by the European Union

2. Oversikt over de vanligste truslene

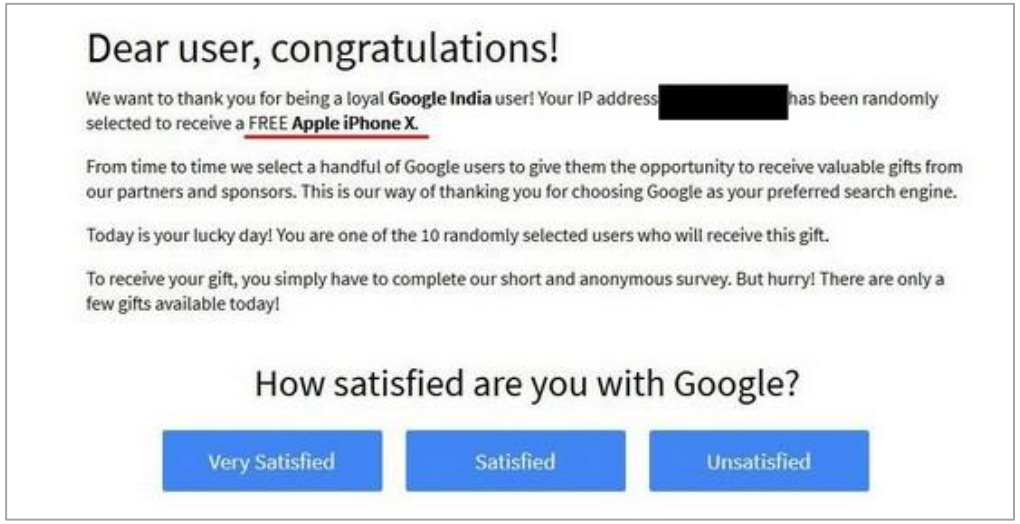
2.4. Sosial manipulering

Med sosial manipulering menes bruk av sosiale taktikker for å utnytte ansattes tillit, uaktsomhet eller uvitenhet for å få tak i konfidensiell informasjon. Selv om phishing- og skadevareangrep ofte utnytter disse sårbarhetene og **overlapper** med sosial manipulering, bruker ren sosial manipulering mer direkte sosiale **taktikker,** og kan omfatte følgende:

Baiting

Baiting baserer seg på **nysgjerrighet eller grådighet** for å lokke folk til å laste ned skadelige filer eller besøke kompromitterte nettsteder. Angriperne tilbyr **fristende lokkemat,** for eksempel gratis nedlasting av programvare, filmer eller gavekort, som inneholder skadevare eller fører til phishing-sider når de åpnes.

Baiting er ofte knyttet til en eller annen form for pretexting, spear phishing, imitasjon osv. for å ramme brukerens **sårbarheter** og øke avsenderens **troverdighet**.



Kilde: Dummies.com

2. Oversikt over de vanligste truslene

2.4. Sosial manipulering

Med sosial manipulering menes bruk av sosiale taktikker for å utnytte ansattes tillit, uaktsomhet eller uvitenhet for å få tak i konfidensiell informasjon. Selv om phishing- og skadevareangrep ofte utnytter disse sårbarhetene og **overlapper** med sosial manipulering, bruker ren sosial manipulering mer direkte sosiale **taktikker,** og kan omfatte følgende:

Tailgating (Piggybacking):

Tailgating, eller piggybacking, innebærer at man **fysisk skaffer seg uautorisert tilgang** til begrensede områder eller systemer ved å følge etter en autorisert person.

Angripere utnytter **menneskelig høflighet eller manglende bevissthet** til å ta seg inn i sikrede lokaler uten tillatelse.

"Watering hole attack"

Vannhullsangrep retter seg mot bestemte grupper eller organisasjoner ved å **infisere nettsteder som medlemmene besøker,** med skadevare.

Angripere kompromitterer legitime nettsteder for å **distribuere skadevare** til intetanende besøkende og utnytter deres tillit til det kompromitterte nettstedet.

Etterligning (identitetstyveri):

De fleste phishing-taktikker innebærer en eller annen form for etterligning. Men noen inkluderer tilleggselementer for å øke troverdigheten, som utgjør **identitetstyveri**.

Disse kan omfatte stjålne eller forfalskede legitimasjoner og dokumenter, IA-skapte elementer osv. for å **villede** om deres autentisitet.

Co-funded by the European Union

2. Oversikt over de vanligste truslene

2.4. Sosial manipulering

Sosial manipulering er ofte en inngangsport for å levere malware eller få ofrene til å utføre en handling. Noen tall fra **2023** viser hvor utbredt, sofistikert og farlig sosial manipulering er (Kilde: Resmo).

90 %

90 % av alle datainnbrudd og **98 %** av alle dataangrep (vellykkede eller ikke) hadde elementer av sosial manipulering.

$4.5 M

Datainnbrudd som ble initiert ved hjelp av sosial manipulering, **kostet i** gjennomsnitt **over 4,5 millioner dollar**.

700

En typisk organisasjon (i USA) utsettes **årlig for** over **700 sosial manipulering-angrep.**

+ 354 %

Kontoovertakelsesangrep økte med 354 % i 2023 sammenlignet med året før.

Co-funded by the European Union

SociALL

3. Forebyggende tiltak

1. Passordsikkerhet
2. Tofaktorautentisering (2FA)
3. Anti-virus
4. Programvareoppdateringer
5. Nettverkssikkerhet
6. Sikkerhetskopiering av data

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
MPWA
Medicalscan
åpenhet
Co-funded by the European Union

3. Forebyggende tiltak

3.1. Passordsikkerhet

Hvorfor er det viktig?

Passordsikkerhet er den **første svakheten som** utnyttes av nettkriminelle. **Sterkere** passord (dvs. mer kompliserte og varierte) er vanskeligere å gjette eller avdekke ved hjelp av brute-force-angrep, og kan derfor være et nyttig **førsteforsvar** mot nettangrep.

Hva kan jeg gjøre?

- Angi **sterke** passord: minst **16** tegn, med store og små bokstaver, tall og spesialtegn.
- **Endre setninger** til passord i stedet for ord, ved hjelp av en kode for å forvandle ulike typer bokstaver. F.eks. "Icàre@b0utSecur1ty!".
- Bruk **passordadministratorer som** husker passordene dine for deg og genererer passord.

Hva kan organisasjonen min gjøre?

- Konfigurer systemene dine (e-post, elektroniske meldingsverktøy, ERP, CRM osv.) slik at brukerne må **fornye passordet regelmessig.** Dette vil forkorte tiden et gitt passord er gyldig.
- Konfigurer **passordregler** for å sikre at brukerne ikke bruker **samme passord to ganger,** og at passordet er **sterkt nok**.
- Fremtving en generell **passordfornyelse** etter et sikkerhetsbrudd.

Co-funded by the European Union

3. Forebyggende tiltak

3.1. Passordsikkerhet

Hvorfor er det viktig?

Passordsikkerhet er den **første svakheten som** utnyttes av nettkriminelle. **Sterkere** passord (dvs. mer kompliserte og varierte) er vanskeligere å gjette eller avdekke ved hjelp av brute-force-angrep, og kan derfor være et nyttig **førsteforsvar** mot nettangrep.

Passordadministratorer

- Passordadministratorer **lagrer passordene dine** og gjør at du slipper å huske dem. Som skyløsninger er de **tilgjengelige fra andre enheter**.
- Registrering av passord kan gjøres **manuelt** eller **automatisk.** Du kan også angi at passordadministratoren skal fylle ut passordfeltet automatisk når du kobler til kontoene dine.
- Det beste er at passordadministratorer kan **generere unike, svært sterke passord** for alle kontoene dine og huske dem for deg. Du trenger ikke engang å kunne dem.
- Alt du trenger å huske, er **ett svært sterkt passord** - det som gir deg tilgang til passordadministratoren.

Nyttige verktøy

- Dashlane
- 1Lösenord
- LastPass
- Bitwarden

Co-funded by the European Union

3. Forebyggende tiltak

3.2. Tofaktorautentisering (2FA)

SociALL

Hvorfor er dette viktig?

2FA forbedrer sikkerheten drastisk: Denne autentiseringsmetoden krever bruk av minst **to enheter** for å logge inn på en konto, og begge må være **registrert** og **klarert på** forhånd. Denne metoden gir ikke bare brukeren **kontroll** over en konto som kan ha blitt kompromittert, men kan også **indikere** at den har blitt det.

Hva kan jeg gjøre?

- **Aktiver 2FA** så tidlig som mulig - når et passord eller en konto først er kompromittert, er det for sent.
- I de fleste programvarer og nettsteder finner du muligheten til å aktivere 2FA under **Innstillinger > Sikkerhet** (IOS og Microsoft, Google-tjenester, sosiale medier osv.).
- Den mest brukte og pålitelige metoden er bruk av **to enheter som** tilhører brukeren (f.eks. telefon og datamaskin) som er registrert på en konto.

Hva kan organisasjonen min gjøre?

- For de fleste systemer kan IT-avdelingen håndheve **2FA i hele systemet** for alle brukere. 2FA kan også kalles "totrinnsverifisering" eller "flerfaktorautentisering".
- Dette krever imidlertid at alle **ansatte har tilgang til to enheter**, ideelt sett kun til profesjonell bruk, noe som kanskje ikke er tilfelle. Alternativt kan de ansatte **oppfordres** til å aktivere 2FA.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
MPA
Medical Scan
åpenhet
Co-funded by the European Union

3. Forebyggende tiltak

3.2. Tofaktorautentisering (2FA)

Hvorfor er det viktig?

2FA forbedrer sikkerheten drastisk: Denne autentiseringsmetoden krever bruk av minst **to enheter** for å logge inn på en konto, og begge må være **registrert** og **klarert på** forhånd. Denne metoden gir ikke bare brukeren **kontroll** over en konto som kan ha blitt kompromittert, men kan også **indikere** at den har blitt det.

Hvordan gjør jeg det?

- Google Workspace (Gmail, Gdrive, Kalender osv.)
- Microsoft 365 (Outlook, OneDrive, Teams osv.)
- Slack
- Zoom

Og andre - generelt tilgjengelig i **sikkerhetsfanen i Innstillinger** for de fleste digitale verktøy - også til personlig bruk (sosiale medier, bankvirksomhet, e-handel, offentlige applikasjoner, nettsteder osv.)

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medicalscan
åpenhet
Co-funded by the European Union

3. Forebyggende tiltak

3.3. Anti-virus

Hvorfor er det viktig?

Anti-virus beskytter eieren ved å **skanne potensielle trusler og oppdage risikoer**, fra phishing via e-post eller forsøk på skadelig programvare til falske nettsteder og programmer. Denne beskyttelsen omfatter også **eksterne enheter som** samhandler med datamaskinen, for eksempel USB-minnepinner som også kan inneholde skadelig programvare.

Hva kan jeg gjøre?

- **Installer** antivirusprogramvare på **egen hånd** hvis den ikke leveres av organisasjonen (eller be **om** at det gjøres i hele organisasjonen). Ubeskyttede datamaskiner er **lette mål** for cyberkriminelle.
- Husk at antivirus er et ekstra lag av en **sikkerhet som fortsatt avhenger av den menneskelige** faktoren: Vær **like årvåken på** nettet uansett om du er "beskyttet" eller ikke.

Hva kan organisasjonen min gjøre?

IT-avdelingen kan og **bør** installere, konfigurere og administrere oppdateringer av **antivirusprogramvare for hele systemet for** å sikre at organisasjonens digitale sikkerhet er bedre beskyttet.

Nyttige verktøy

ESET
Bitdefender
Kaspersky
AVG

Co-funded by the European Union

3. Forebyggende tiltak

3.4. Programvareoppdateringer

Hvorfor er det viktig?

Ved å holde programvare og operativsystemer **oppdatert** hindrer man cyberkriminelle i å utnytte kjente **sikkerhetsproblemer**: Programvareleverandører stresstester jevnlig sin egen sikkerhet. Når de oppdager potensielle sikkerhetsbrudd, legger de **ut oppdateringer som** fjerner sårbarhetene eller gjør dem ubrukelige.

Hva kan jeg gjøre?

Ikke utsett oppdateringen av all programvare og alle applikasjoner du bruker (privat og profesjonelt) når du mottar et oppdateringsvarsel. Kontroller regelmessig at alt er oppdatert i applikasjonssenteret ditt.

Hva kan organisasjonen min gjøre?

IT-avdelingen kan konfigurere automatiske oppdateringer for operativsystemer og applikasjoner som brukes i hele organisasjonen, og velge når og hvor ofte de skal installeres uten å forstyrre driften.

Hvordan gjør jeg det?

På Windows

På Mac

På Android

På IOS

Nyttige verktøy

Administrer oppdateringer i Windows

Slå på automatiske appoppdateringer

Oppdater MacOS på Mac

Co-funded by the European Union

3. Forebyggende tiltak

3.5. Nettverkssikkerhet - VPN

Hvorfor er det viktig?

Når det er nødvendig for de ansatte å få tilgang til informasjon **utenfor lokalene**, blir det vanskeligere for IT-avdelingen å ha **kontroll over alle sikkerhetsaspekter**. **Virtuelle private nettverk (VPN) gjør det** mulig å opprette et **direkte, sikkert og isolert nettverk** mellom to maskiner, slik at de kan samhandle og utveksle data.

Hvordan fungerer det?

Et VPN er en teknologi som skaper en **sikker og kryptert** forbindelse over Internett. VPN-er krypterer data som overføres mellom brukerens enhet og VPN-serveren, slik at tredjeparter ikke får tilgang til dataene. Denne krypteringen er et **ekstra sikkerhetslag som** sikrer at sensitiv informasjon som passord, kredittkortopplysninger og personlig kommunikasjon forblir sikker.

Når det gjelder omsorgsarbeidere, vil et VPN for det meste **sikre ekstern tilgang** til private nettverk og ressurser, for eksempel bedriftens intranett, servere eller databaser, særlig for dem som jobber ute i feltet. De vil også gi **økt sikkerhet** for dem som kobler seg til Internett via **offentlige** og generelt usikrede **Wifi-nettverk**.

Co-funded by the European Union

3. Forebyggende tiltak

3.5. Nettverkssikkerhet - VPN

Hvorfor er det viktig?

Når det er nødvendig for de ansatte å få tilgang til informasjon **utenfor lokalene**, blir det vanskeligere for IT-avdelingen å ha **kontroll over alle sikkerhetsaspekter**. **Virtuelle private nettverk (VPN) gjør det** mulig å opprette et **direkte, sikkert og isolert nettverk** mellom to maskiner, slik at de kan samhandle og utveksle data.

Hva kan organisasjonen min gjøre?

VPN bør installeres av **organisasjonens tekniske avdeling** når det er behov for det, ettersom det for det meste vil bli brukt som en **systemomfattende geografisk utvidelse av det eksisterende nettverket**, noe som hindrer den enkelte bruker i å installere det på egen hånd. Enkeltpersoner kan imidlertid anbefale bruken av et VPN overfor IT-avdelingen eller ledelsen.

VPN kan kreve **installasjon av programvare** på maskinene som skal kobles sammen, samt en **autentiseringsmetode** før tilgang til nettverket. De kan konfigureres slik at de bare fungerer på visse enheter, på visse steder og til visse tider for å begrense ekstern tilgang, samtidig som de ansatte som trenger det, får tilgang til nødvendige data.

Co-funded by the European Union

3. Forebyggende tiltak

3.6. Sikkerhetskopiering av data

Hvorfor er det viktig?

En av de største truslene ved cyberangrep er **endring av sensitive data**, spesielt pasientdata. Det er derfor svært viktig å sørge for sikkerheten og integriteten til disse dataene, selv i møte med en cybertrussel. En robust **institusjonell strategi for sikkerhetskopiering av data**, med regelmessige **sikkerhetskopieringsprosedyrer** og **høyt samsvar blant de ansatte,** er nøkkelen til å sikre dataintegriteten.

Hva kan jeg gjøre?

- Det første tiltaket for å sikre dataintegritet og datasikkerhet er at den enkelte medarbeider følger **de ulike protokollene som er** fastsatt av den tekniske avdelingen, **gjennomgår regelmessig opplæring** og ser alvoret i cybersikkerhet.
- Som sikkerhetsaktør i din egen organisasjon kan du også **spørre** om strategien for sikkerhetskopiering av data, **foreslå** og **argumentere for** endringer.

Hva kan organisasjonen min gjøre?

Det er den tekniske avdelingens ansvar å utforme og implementere en **strategi for sikkerhetskopiering av institusjonens data.** En slik strategi bør omfatte **tiltak for å sikre at de ansatte overholder kravene**, prosedyrer for **regelmessig sikkerhetskopiering av data** på en **skybasert lagringsløsning** (Gdrive, Onedrive osv.) eller en **nettverkstilknyttet lagringsløsning som** gir et sikkerhetsnett for **rask gjenoppretting av data i** tilfelle brudd på dataintegriteten.

Co-funded by the European Union

SociALL

4. Beste praksis og gode vaner

1. Fysisk plass
2. Sikker surfing
3. Sikker e-post
4. Sikker bruk av sosiale medier
5. Sikkerhet for mobile enheter
6. Passordsikkerhet

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
MPWA
Medicalscan
åpenhet
Co-funded by the European Union

4. Beste praksis og gode vaner

4.1. Fysisk plass

Cybersikkerhet starter offline: Før du setter opp tekniske forsvarsverk, må du sørge for å organisere det fysiske rommet på en sikker måte som reduserer farer og sårbarheter.

1. Lås enhetene dine når de ikke er i bruk
2. Sikre arbeidsområdet ditt mot uautorisert tilgang
3. Vedta en policy for rent skrivebord
4. Bruk personvernskjermer
5. Makuler sensitive dokumenter
6. Ikke skriv ned passord
7. Vær oppmerksom på skuldersurfing
8. Aktiver fulldiskkryptering

Co-funded by the European Union

4. Beste praksis og gode vaner

4.1. Fysisk plass

Cybersikkerhet starter offline: Før du setter opp tekniske forsvarsverk, må du sørge for å organisere det fysiske rommet på en sikker måte som reduserer farer og sårbarheter.

1. Lås enhetene dine når de ikke er i bruk

Lås alltid datamaskinen, nettbrettet eller telefonen din når de ikke er i bruk, spesielt på offentlige eller delte steder. Bruk sterke passord, PIN-koder eller biometrisk autentisering (f.eks. fingeravtrykk eller ansiktsgjenkjenning) for å sikre enhetene dine og forhindre uautorisert tilgang.

Tips

- I Windows bruker du snarveien Windows + L for å låse skjermen.
- På Mac bruker du snarveien Control-Command-Q for å låse skjermen.

2. Sikre arbeidsområdet ditt mot uautorisert tilgang

- Hold arbeidsområdet **fritt for uvedkommende**. Sørg for at fysiske adgangspunkter, som dører, vinduer og inngangspartier er sikret og overvåket for å hindre at uvedkommende får adgang til arbeidsområdet eller lokalene.
- **Lås** skuffer, skap eller arkivskap som inneholder sensitive dokumenter, enheter eller lagringsmedier når de ikke er i bruk.
- Sikre **eksterne enheter** som tastaturer, mus og eksterne lagringsenheter (USB, harddisk osv.) og oppbevar dem i låste skuffer eller skap.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medicalscan
åpenhet
Co-funded by the European Union

4. Beste praksis og gode vaner

4.1. Fysisk plass

Cybersikkerhet starter offline: Før du setter opp tekniske forsvarsverk, må du sørge for å organisere det fysiske rommet på en sikker måte som reduserer farer og sårbarheter.

3. Vedta en policy for rent skrivebord

Hold skrivebordet **rent** ved å fjerne sensitive dokumenter, notater og passord fra skrivebordet når du ikke er til stede. Oppbevar fysiske dokumenter på en sikker måte, helst i låste skap eller skuffer.

Tips

En god praksis er å etterstrebe et "0-papir-skrivebord", med kun de papirene som brukes for øyeblikket på skrivebordet. I tillegg til at det beviselig øker effektiviteten og reduserer stress, reduserer det også risikoen for at viktig informasjon blir liggende synlig for uvedkommende.

4. Bruk personvernskjermer

Bruk **personvernskjermer eller -filtre** på datamaskiner eller mobile enheter for å hindre at uvedkommende ser på skjermen din. Personvernskjermer tvinger seerne til å være nøyaktig foran enheten og forhindrer skuldersurfing. De er innebygd i enkelte enheter eller kan lastes ned.

Tips

- På datamaskiner med innebygde personvernskjermer trykker du på F12 eller Fn + D for å aktivere den.
- På Android er de best rangerte appene for personvernskjermer 1) Privacy Screen, 2) Screen Guard Privacy, 3) Privacy filter

Co-funded by the European Union

4. Beste praksis og gode vaner

4.1. Fysisk plass

Cybersikkerhet starter offline: Før du setter opp tekniske forsvarsverk, må du sørge for å organisere det fysiske rommet på en sikker måte som reduserer farer og sårbarheter.

5. Makuler sensitive dokumenter

Makuler eller kast fysiske dokumenter som inneholder sensitiv informasjon, f.eks. finansielle dokumenter, personlig identifikasjon osv. på en **sikker måte** før du kaster dem. Ikke bare kast dem i søpla uten i det **minste å rive i stykker** et dokument.

Tips

Selv om resirkulering er alle ansattes ansvar i dag, må du huske at løst papir ofte blir liggende uten tilsyn før det resirkuleres, og det kan gjøre organisasjonen sårbar for potensielle sikkerhetsbrudd hvis det er sensitivt.

6. Ikke skriv ned passord

Ikke skriv ned passord eller PIN-koder på klistrelapper, notatbøker eller fysiske dokumenter. Hvis det er absolutt nødvendig å skrive ned et passord, gjør det på et sted der det ikke kan bli funnet, og krypter det med en kode som bare du kan tyde (f.eks. antall barn til søsteren/hundens bursdagsmåned osv.).

Tips

Bruk i stedet en anerkjent passordbehandler til å lagre og administrere passord på en sikker måte. Det eneste passordet du trenger å huske, er passordet til passordbehandleren.

Co-funded by the European Union

4. Beste praksis og gode vaner

4.1. Fysisk plass

Cybersikkerhet starter offline: Før du setter opp tekniske forsvarsverk, må du sørge for å organisere det fysiske rommet på en sikker måte som reduserer farer og sårbarheter.

7. Vær oppmerksom på skuldersurfing

Vær oppmerksom på omgivelsene og beskytt skjermen og tastaturet mot innsyn fra uvedkommende, spesielt på offentlige steder. Beskytt tastaturet når du **taster** inn PIN-koder eller passord på minibanker, tastaturer eller mobile enheter.

Tips

- Personvernskjermer er en god måte å bekjempe skuldersurfing på.
- Når du befinner deg i et offentlig rom, bør du helst sitte med ryggen mot en vegg for å unngå skuldersurfing bakfra.

8. Aktiver fulldiskkryptering

Aktiver **fulldiskkryptering** på enhetene dine for å beskytte data som er lagret på enhetens harddisk eller lagringsmedier. Dette sikrer at uautoriserte brukere ikke får tilgang til dataene uten krypteringsnøkkelen, selv om enheten blir stjålet eller går tapt.

Tips

- I Windows aktiverer du kryptering under Innstillinger > Personvern og sikkerhet.
- De fleste mobiloperativsystemer har nå også funksjoner som gjør det mulig å fjernslette data hvis du mister enheten.

Co-funded by the European Union

4. Beste praksis og gode vaner

4.2. Sikker surfing

Når du **surfer** på Internett, må du sørge for å opprettholde følgende beste praksis.

1. Bruk sikre nettsteder (HTTPS)
2. Hold programvare og operativsystem oppdatert
3. Bruk annonseblokkere og innholdsfiltre
4. Vær forsiktig med nedlastinger
5. Bla anonymt
6. Tøm regelmessig nettleserens hurtigbuffer og informasjonskapsler

Co-funded by the European Union

4. Beste praksis og gode vaner

4.2. Sikker surfing

Når du **surfer** på Internett, må du sørge for å opprettholde følgende beste praksis.

1. Bruk sikre nettsteder (HTTPS)

Se etter **HTTPS** i nettadressen for å sikre en sikker tilkobling når du overfører sensitiv informasjon, for eksempel påloggingsinformasjon eller finansielle opplysninger. Unngå å oppgi personopplysninger på nettsteder som kun bruker **HTTP**.

Tips

HTTP-meldinger er i klartekst, noe som betyr at uvedkommende enkelt kan få tilgang til og lese dem over Internett. HTTPS overfører alle data i kryptert form. Når brukere sender sensitive data, kan ingen tredjeparter snappe opp dataene over nettverket.

2. Hold programvare og operativsystem oppdatert

Oppdater jevnlig operativsystemet (OS), nettleseren, antivirusprogrammet og andre programmer for å forhindre kjente sårbarheter og beskytte mot sikkerhetstrusler.

Tips

Ikke utsett oppdateringen av all programvare og alle applikasjoner du bruker (privat og profesjonelt) når du mottar et oppdateringsvarsel. Kontroller regelmessig at alt er oppdatert i applikasjonssenteret ditt.

Co-funded by the European Union

4. Beste praksis og gode vaner

4.2. Sikker surfing

Når du **surfer** på Internett, må du sørge for å opprettholde følgende beste praksis.

3. Bruk annonseblokkere og innholdsfiltre

Installer **annonseblokkere og innholdsfiltre** for å hindre at ondsinnede annonser, popup-vinduer eller skript ødelegger surfeopplevelsen din eller leverer malware. Enkelte nettsteder kan kreve at du deaktiverer den for å få tilgang til innhold, noe som enkelt kan gjøres fra ikonet i nettleseren.

Tips

Best rangerte gratis adblockere:

- uBlock opprinnelse
- Privatlivets fred Badger
- Ghostery
- Adblock plus

4. Vær forsiktig med nedlastinger

Last ned programvare, filer og vedlegg kun fra **anerkjente kilder,** og unngå å laste ned innhold fra upålitelige nettsteder eller ukjente kilder for å minimere risikoen for skadevareinfeksjoner.

Tips

Det finnes utrolig mye innhold tilgjengelig på Internett. Hvis et nettsted krever at du laster ned noe, kan du sannsynligvis få tilgang til tilsvarende innhold fra et annet nettsted uten å laste ned noe.

Co-funded by the European Union

4. Beste praksis og gode vaner

4.2. Sikker surfing

Når du **surfer** på Internett, må du sørge for å opprettholde følgende beste praksis.

5. Bla gjennom anonymt

Vurder å bruke et **virtuelt privat nettverk (VPN)** for å **kryptere** internettrafikken din og surfe anonymt, spesielt når du bruker offentlige Wi-Fi-nettverk eller får tilgang til sensitiv informasjon.

Tips

Ikke forveksle "inkognitomodus" eller "privat surfing"-modus med et VPN: de gjør ikke surfingen din tryggere: de sletter bare nettleserhistorikken din fra enheten. Men nettleserhistorikken din er fortsatt synlig for omverdenen, i tillegg til IP-adressen din, nettverket ditt osv.

6. Tøm regelmessig nettleserens hurtigbuffer og informasjonskapsler

Tøm med jevne mellomrom nettleserens hurtigbuffer, informasjonskapsler og nettleserhistorikk for å fjerne **sporingsdata** og minimere risikoen for at uvedkommende får tilgang til surfevanene dine eller personopplysninger.

Tips

I Chrome klikker du på de tre prikkene øverst til høyre > Slett nettleserdata. I den nye fanen som åpnes, velger du perioden du vil slette data for (ideelt sett "Hele tiden"), velger de tre alternativene (nettleserhistorikk, informasjonskapsler og hurtigbuffer) og klikker på "Slett nettleserdata" for å tømme nettleseren med én gang.

Co-funded by the European Union

4. Beste praksis og gode vaner

4.3. Sikker e-post

Når du mottar en e-post, bør du stille deg selv følgende spørsmål for å unngå sikkerhetsproblemer:

1. Kjenner jeg igjen avsenderen?
2. Er e-posten uventet eller uoppfordret?
3. Henvender e-posten seg til meg med navn?
4. Er det stave- eller grammatikkfeil?
5. Finnes det mistenkelige vedlegg?
6. Inneholder e-posten uventede lenker?
7. Ber e-posten om sensitiv informasjon?
8. Ser signaturen og kontaktinformasjonen ekte ut?
9. Har jeg et eksisterende forhold til avsenderen?
10. Bruker e-posten trusler eller frykttaktikk?
11. Oppdaget antivirusprogrammet noe mistenkelig?
12. Ser den ut som andre e-poster fra denne leverandøren?

Sørg i tillegg for å alltid behandle en e-post med følgende **holdning**:

- Du må **aldri iverksette umiddelbare, forhastede tiltak.**
- **Gå alltid ut fra** at en e-post kan være **svindel**, ta deg tid til å studere og "klarere" den.
- **Stol på dømmekraften** og instinktene **dine**: Hvis noe føles rart, bør du utforske det med forsiktighet.
- Husk at svindlere spiller på **følelser** som frykt, gjennom skremsler og trusler. Hold **hodet kaldt** og behold **roen** i alle tilfeller.

Co-funded by the European Union

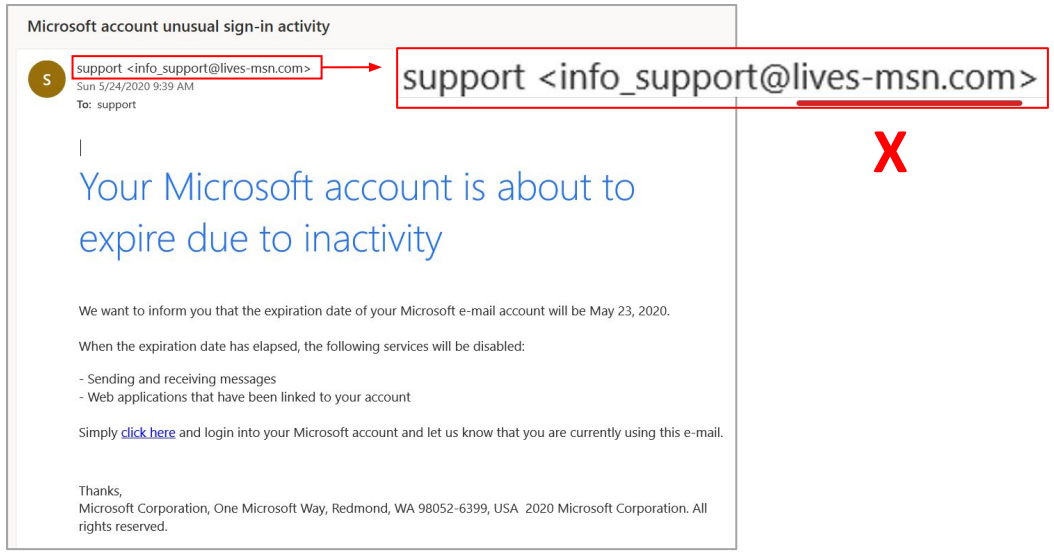
4. Beste praksis og gode vaner

4.3. Sikker e-post

Når du mottar en e-post, bør du stille deg selv følgende spørsmål for å unngå sikkerhetsproblemer:

1. Kjenner jeg igjen avsenderen?

Bekreft avsenderens identitet, ikke bare ved å se navnet som vises øverst og i signaturen, men også den **faktiske e-postadressen** som sendte e-posten.



2. Er e-posten uventet eller uønsket?

Vær på vakt mot uventede e-poster, spesielt de som krever at du gjør noe **raskt** eller tilbyr **uoppfordrede tjenester**. Svindlere bruker ofte slike e-poster til å lure mottakere, oftest med disse temaene:

- Behov for å oppdatere eller verifisere kontoinformasjon (kontosuspensjon, utløp, sikkerhetsvarsel osv.).
- Behov for å betale en ventende faktura via en lenke.
- Tilbud om falske jobbmuligheter.
- Betaling eller fjerntilgang til datamaskin eller konto på forespørsel fra "support" for å løse tekniske problemer.
- Begov for å betale behandlingsgebyr eller oppgi personopplysninger for å få en uoppfordret belønning eller premie.

Co-funded by the European Union

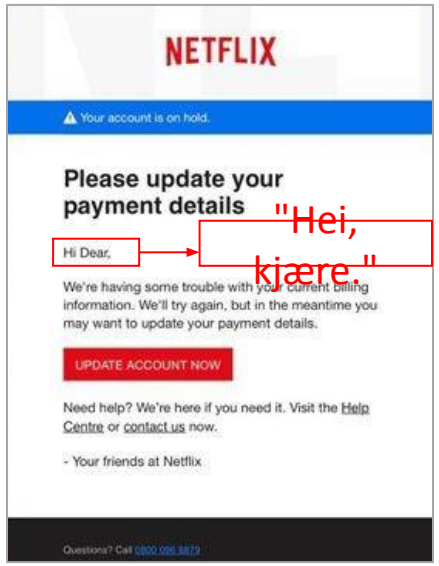
4. Beste praksis og gode vaner

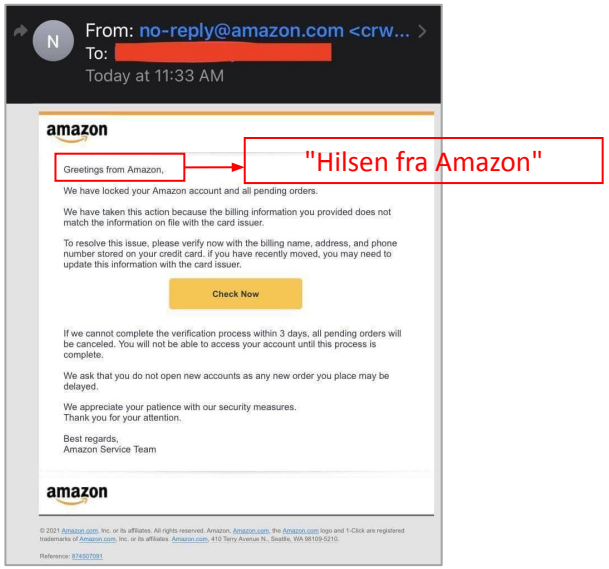
4.3. Sikker e-post

Når du mottar en e-post, bør du stille deg selv følgende spørsmål for å unngå sikkerhetsproblemer:

3. Henvender e-posten seg til meg med navn?

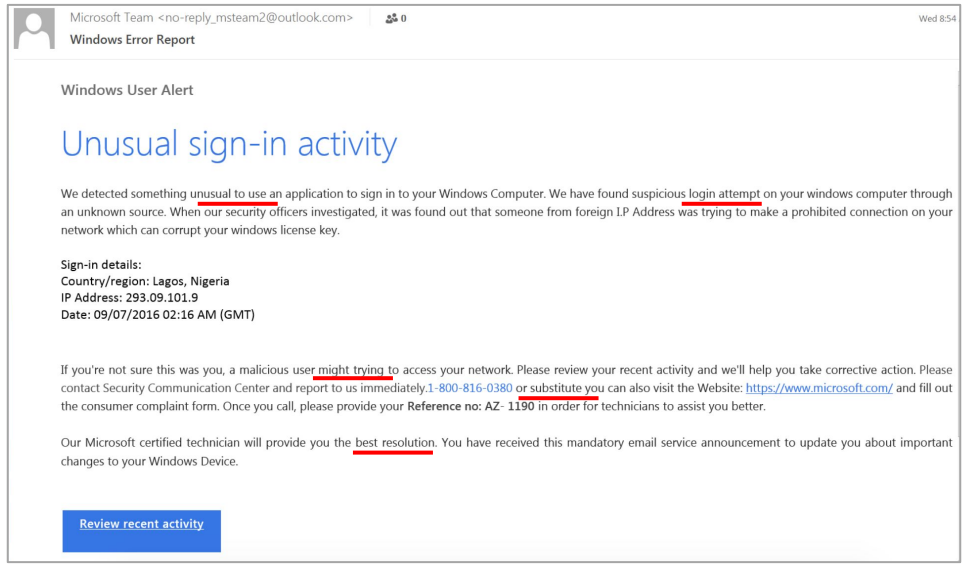
Legitime organisasjoner bruker ofte navnet ditt i sin kommunikasjon. **Generiske hilsener** eller **feilstaving** av navnet ditt kan være et rødt flagg.





4. Er det stave- eller grammatikkfeil?

Dårlig skrevne e-poster med **stave-** og **grammatikkfeil** kan tyde på forsøk på phishing. Legitime organisasjoner gjør generelt færre feil i e-postene sine.



JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medicalscar
åpenhet
Co-funded by the European Union

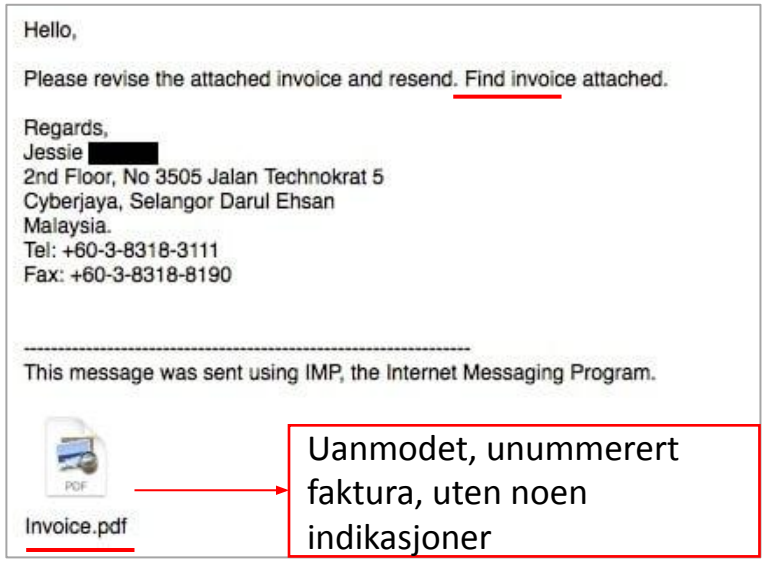
4. Beste praksis og gode vaner

4.3. Sikker e-post

Når du mottar en e-post, bør du stille deg selv følgende spørsmål for å unngå sikkerhetsproblemer:

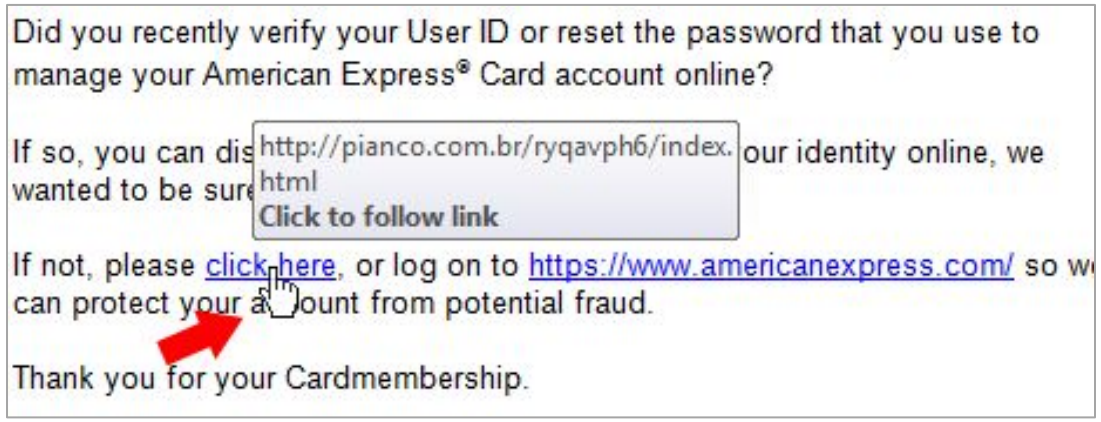
5. Finnes det mistenkelige vedlegg?

Unngå å åpne **uventede vedlegg**, spesielt fra ukjente kilder. Ondsinnede vedlegg kan inneholde skadelig **programvare** eller forsøk på **phishing.**



6. Inneholder e-posten uventede lenker?

Hold musepekeren over eventuelle lenker i e-posten uten å klikke for å se den **faktiske nettadressen**. Hvis lenken ikke samsvarer med avsenderens offisielle nettsted eller ser mistenkelig ut, kan det være et forsøk på phishing.



JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medicalscan
åpenhet
Co-funded by the European Union

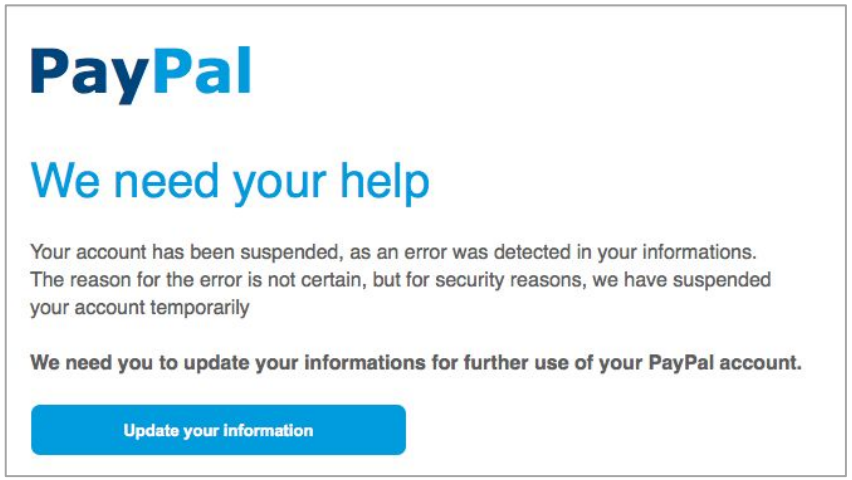
4. Beste praksis og gode vaner

4.3. Sikker e-post

Når du mottar en e-post, bør du stille deg selv følgende spørsmål for å unngå sikkerhetsproblemer:

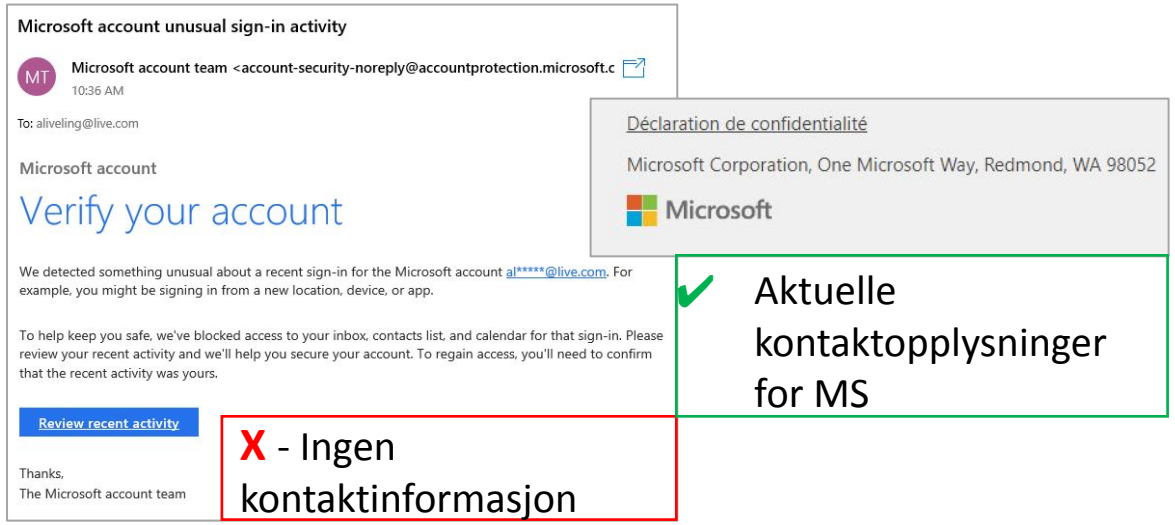
7. Ber e-posten om sensitiv informasjon?

Organisasjoner **ber** vanligvis **ikke om sensitiv informasjon** via **e-post** eller **lenke** (for eksempel passord eller kredittkortopplysninger), men ber deg normalt om å koble deg til **kontoen din** på nettstedet deres.



8. Ser signaturen og kontaktinformasjonen ekte ut?

Legitime organisasjoner oppgir vanligvis **tydelig kontaktinformasjon** i e-postene sine, inkludert en **fysisk adresse**. Kontroller avsenderens opplysninger, inkludert **signaturen,** og kryssjekke dem med offisielle kilder.



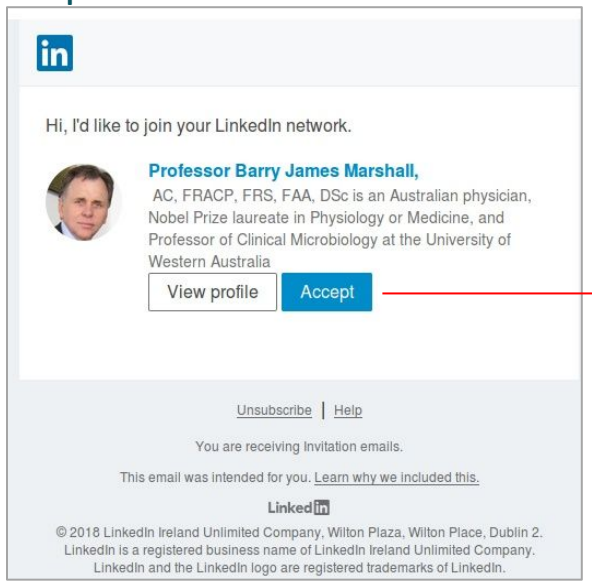
4. Beste praksis og gode vaner

4.3. Sikker e-post

Når du mottar en e-post, bør du stille deg selv følgende spørsmål for å unngå sikkerhetsproblemer:

9. Har jeg et eksisterende forhold til avsenderen?

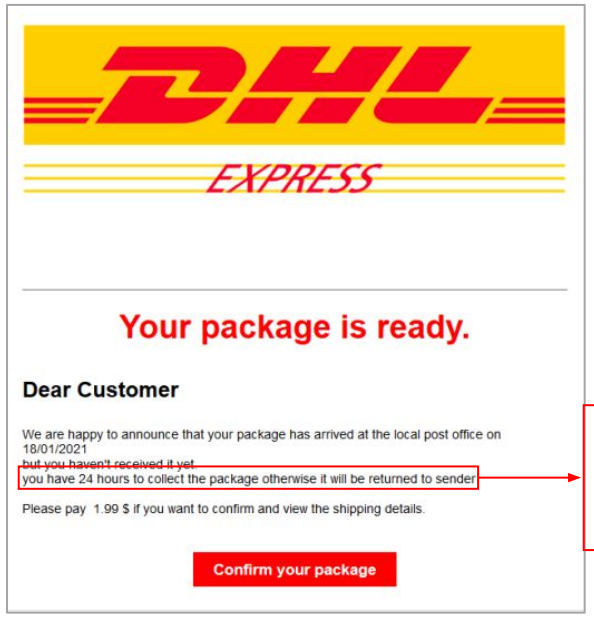
Hvis e-posten hevder å komme fra en organisasjon du har en konto hos, bør du verifisere informasjonen **fra kontoen din i** stedet for å stole utelukkende på e-posten.



Sjekk LinkedIn-kontoen i stedet for å klikke på "Godta".

10. Brukes det trusler eller frykt i e-posten?

Svindlere bruker **trusler** eller frykttaktikker for å presse mottakerne til å handle raskt. Vær på vakt mot e-poster som skaper en følelse av **hastverk** eller **frykt**.



"Du har 24 timer på deg til å hente pakken, ellers vil den bli returnert til avsender."

Co-funded by the European Union

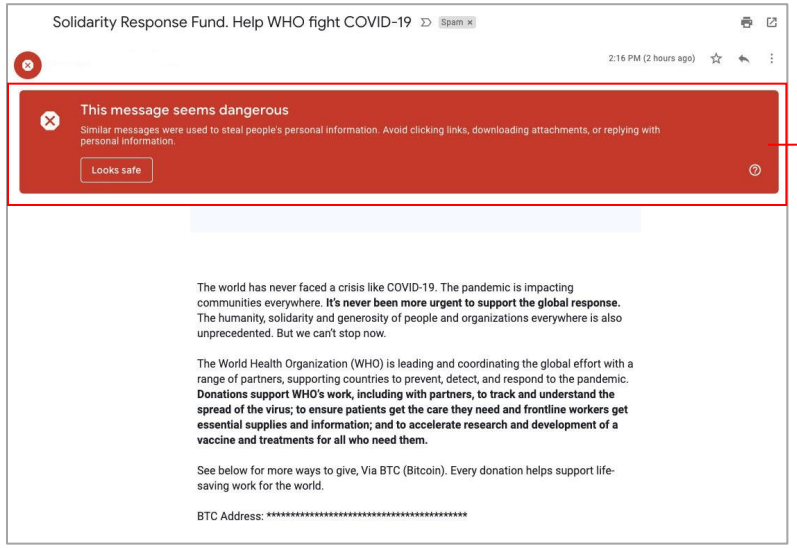
4. Beste praksis og gode vaner

4.3. Sikker e-post

Når du mottar en e-post, bør du stille deg selv følgende spørsmål for å unngå sikkerhetsproblemer:

11. Oppdaget antivirusprogrammet noe mistenkelig?

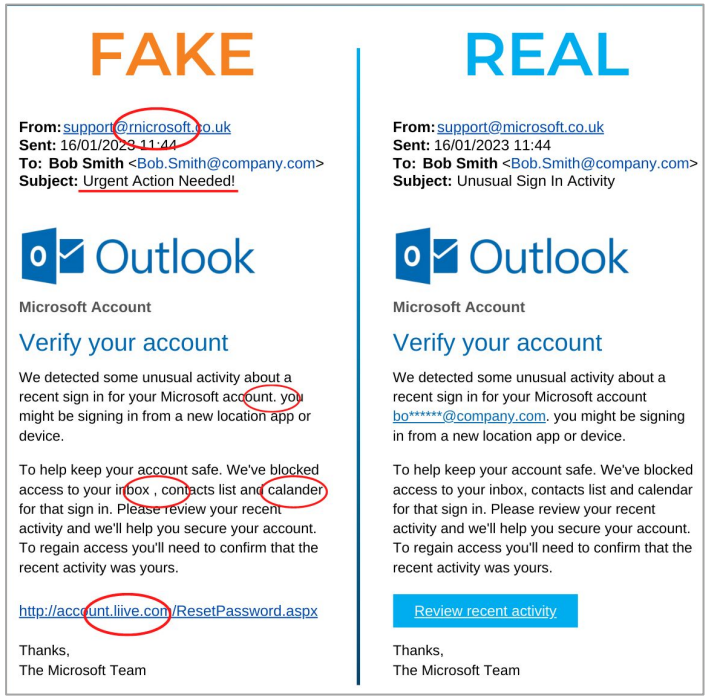
De fleste e-postleverandører har **innebygde moduler som oppdager** forsøk på phishing. Dessuten kan ditt eget **antivirusprogram** ha flagget e-posten som **mistenkelig**. I så fall bør du være **forsiktig med** e-posten.



"Denne meldingen virker farlig"

12. Ser den ut som andre e-poster fra denne leverandøren?

Når du mottar en e-post fra en organisasjon du **allerede har mottatt e-post** fra, bør du kontrollere at design, varemerke, kontaktinformasjon, opphavsrett, lenker og språk **stemmer overens** før du stoler på den.



JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medical car
åpenhet
Co-funded by the European Union

4. Beste praksis og gode vaner

4.4. Sikker bruk av sosiale medier

Bruk sosiale medier på en trygg måte ved å integrere følgende fremgangsmåter.

1. Gå gjennom og juster personverninnstillingene
2. Vær selektiv med venneforespørsler og forbindelser
3. Se opp for phishing og svindel
4. Vær oppmerksom på deling av plassering og hva du legger ut.
5. Bekreft kontoens autentisitet
6. Overvåk tredjepartsapper og tillatelser

Co-funded by the European Union

4. Beste praksis og gode vaner

4.4. Sosiale medier og meldinger

Bruk sosiale medier på en trygg måte ved å integrere følgende fremgangsmåter.

1. Gå gjennom og juster personverninnstillingene

Gå jevnlig **gjennom og juster personverninnstillingene dine** på sosiale medier for å kontrollere hvem som kan se innleggene, personopplysningene og bildene dine. **Begrens målgruppen** for innleggene dine, og vurder å **begrense tilgangen** til sensitiv informasjon til betrodde venner og kontakter.

Tips

De fleste standard personverninnstillinger på sosiale medier kan gjøre det mulig å dele informasjon om deg med andre tredjepartsbrukere på nettet, inkludert navn, alder, bosted, kjønn osv.

2. Vær selektiv med venneforespørsler og forbindelser

Vær forsiktig når du godtar **venneforespørsler eller kontakter** fra ukjente personer. Kontroller identiteten til personen før du godtar forespørselen, spesielt hvis du ikke kjenner vedkommende personlig. Mange svindlere på sosiale medier starter med å bli "vennen din" for å få **tilgang til flere av opplysningene dine**.

Tips

Prøv å verifisere autensiteten av forespørselen på andre måter. Hvis du f.eks. mottar en forespørsel fra noen som hevder å være broren til vennen din, kan du be vennen din om å bekrefte personens identitet før du aksepterer den.

Co-funded by the European Union

4. Beste praksis og gode vaner

4.4. Sosiale medier og meldinger

Bruk sosiale medier på en trygg måte ved å integrere følgende fremgangsmåter.

3. Pass deg for phishing og svindel

Vær **forsiktig med uønskede** meldinger, lenker eller forespørsler fra ukjente personer på sosiale medier. Unngå å **klikke på mistenkelige lenker** eller laste ned vedlegg fra ukjente kilder, da dette kan føre til phishing-svindel eller malware-infeksjoner.

Tips

Mange svindelforsøk på sosiale medier skjer gjennom hacking av kontoen til en av kontaktene dine. Vær forsiktig når en kontakt du kjenner, sender deg uoppfordrede, uvanlige forespørsler (f.eks. om økonomisk støtte til slektninger som ligger på sykehus), og bekreft med vedkommende via et annet medium.)

4. Vær oppmerksom på deling av plassering og hva du legger ut.

Begrens deling av posisjonen din på sosiale medier, spesielt når du legger ut bilder eller oppdateringer i sanntid. Unngå å oppgi nøyaktig hvor du befinner deg, og unngå å dele personlig informasjon som kan sette sikkerheten din i fare.

Tips

Mange typer informasjon kan brukes av nettkriminelle til å forårsake skade. Bortsett fra det åpenbare (navn, alder, kjønn, bosted osv.), kan mange detaljer brukes av nettkriminelle, for eksempel navn på nærmeste skole, tidligere eller nåværende arbeidsplass, skjermbilder med personopplysninger osv.

Co-funded by the European Union

4. Beste praksis og gode vaner

4.4. Sosiale medier og meldinger

Bruk sosiale medier på en trygg måte ved å integrere følgende fremgangsmåter.

5. Bekreft kontoens autentisitet

Vær på vakt mot **falske eller kontoer som etterligner andre kontoer** på sosiale medier, spesielt kontoer som utgir seg for å være kjendiser, offentlige personer eller merkevarer. **Verifiser autensiteten** til kontoer før du samhandler med dem eller deler personlig informasjon.

Tips

Bare i 2021 fjernet Facebook 1,7 milliarder falske kontoer. På samme måte er nesten 1 av 5 (19,42 %) Twitter-håndtak falske eller spam. Det blå krysset som "sertifiserer" en konto, kan så å si hvem som helst få, og er ikke en indikator på at en konto er til å stole på.

6. Overvåk tredjepartsapper og tillatelser

Gå jevnlig **gjennom og administrer tillatelsene** til tredjepartsapper som er koblet til kontoene dine på sosiale medier. Fjern tilgangen til apper du ikke lenger bruker eller stoler på, for å minimere risikoen for misbruk av data eller brudd på personvernet.

Tips

Vær oppmerksom på tillatelsene som gis til disse programmene, fordi de kan gi tilgang til privat informasjon som de ikke bør ha tilgang til.

Co-funded by the European Union

4. Beste praksis og gode vaner

4.5. Sikkerhet for mobile enheter

Bruk **mobilenheten** din på en **tryggere måte** ved å følge følgende fremgangsmåter.

1. Bruk en sikker skjermlås
2. Hold programvaren og operativsystemet oppdatert
3. Krypter data
4. Bruk en pålitelig appbutikk
5. Gå gjennom appers tillatelser
6. Vær forsiktig med offentlig Wifi
7. Aktiver "Finn enheten min"
8. Begrens bruken av Bluetooth og NFC

Co-funded by the European Union

4. Beste praksis og gode vaner

4.5. Sikkerhet for mobile enheter

Bruk **mobilenheten** din på en **tryggere måte** ved å integrere følgende fremgangsmåter.

1. Bruk en sikker skjermlås

Aktiver en **sikker skjermlås** (f.eks. PIN-kode, passord, mønster, biometrisk identifikasjon) for å hindre uautorisert tilgang til enheten hvis den blir mistet eller stjålet. Unngå å bruke mønstre eller PIN-koder som er lette å gjette seg til.

2. Hold programvaren og operativsystemet oppdatert

Oppdater jevnlig **mobiloperativsystemet**, apper og sikkerhetsoppdateringer for å beskytte mot kjente sårbarheter og sikkerhetstrusler. Aktiver automatiske oppdateringer for å sikre at sikkerhetsoppdateringene kommer i tide.

3. Krypter data

Aktiver kryptering av data som er lagret på mobilenheten for å beskytte sensitiv informasjon. De fleste moderne mobile enheter har innebygde krypteringsfunksjoner som krypterer data selv uten at du trenger å gjøre noe.

4. Bruk en pålitelig appbutikk

Last ned apper kun fra **offisielle og pålitelige appbutikker**, som Apples App Store eller Google Play Store, for å minimere risikoen for å laste ned ondsinnede apper eller skadelig programvare.

Co-funded by the European Union

4. Beste praksis og gode vaner

4.5. Sikkerhet for mobile enheter

Bruk **mobilenheten** din på en **tryggere måte** ved å integrere følgende fremgangsmåter.

5. Gå gjennom appers tillatelser

Gå gjennom og administrer apptillatelser for å kontrollere hvilke data og funksjoner apper har tilgang til på enheten. **Deaktiver unødvendige tillatelser** som apper ikke trenger for å fungere.

6. Vær forsiktig med offentlig Wifi

Unngå å koble til **usikrede offentlige Wi-Fi-nettverk**, da de kan være sårbare for avlytting eller man-in-the-middle-angrep. **Bruk et VPN** for å kryptere internettrafikken din når du kobler til offentlige Wi-Fi-nettverk.

7. Aktiver "Finn enheten min"

Aktiver "**Finn min enhet**"- eller "**Finn min iPhone**"-funksjonen på mobilenheter for å fjernlokalisere, låse eller slette enheten hvis den blir stjålet eller mistet. Denne funksjonen bidrar til å beskytte dataene og personvernet ditt ved tyveri eller tap.

8. Begrens bruken av Bluetooth og NFC

Deaktiver Bluetooth og NFC når de ikke er i bruk for å hindre uautorisert tilgang eller sammenkobling med andre enheter. Vær forsiktig når du parer med ukjente enheter, og bruk Bluetooth-enheter fra pålitelige kilder.

Co-funded by the European Union

4. Beste praksis og gode vaner

4.6. Passordsikkerhet

Sikre passordene dine ved å sørge for at de inneholder følgende elementer.

1. Bruk sterke og unike passord
2. Bruk forskjellige passord for hver konto
3. Bruk passordfraser i stedet for ord
4. Bruk en anerkjent passordadministrator
5. Hold alltid passordene konfidensielle
6. Oppdater passord regelmessig

Co-funded by the European Union

4. Beste praksis og gode vaner

4.6. Passordsikkerhet

Sikre passordene dine ved å sørge for at de inneholder følgende elementer.

1. Bruk sterke og unike passord

Lag sterke, komplekse passord som er vanskelige å gjette. Bruk en kombinasjon av store og små bokstaver, tall og spesialtegn. Unngå å bruke informasjon som er lett å gjette, for eksempel navn, fødselsdager eller vanlige ord.

Tips

Noen nettsteder gir deg en indikasjon på hvor sikkert passordet ditt er. Ikke registrer et passord før det er vurdert som "sterkt" av nettstedet eller programvaren. Passordet bør bestå av minst 16 tegn og bestå av ulike typer tegn.

2. Bruk forskjellige passord for hver konto

Ikke bruk samme passord på flere kontoer. Bruk unike passord for hver enkelt nettkonto for å minimere virkningen av et sikkerhetsbrudd på andre kontoer.

Tips

Bruk en passordadministrator for å slippe å huske eller skrive ned passord. Du trenger bare å huske passordet til passordbehandleren.

Co-funded by the European Union

4. Beste praksis og gode vaner

4.6. Passordsikkerhet

Sikre passordene dine ved å sørge for at de inneholder følgende elementer.

3. Bruk passordfraser i stedet for ord

Vurder å bruke **passordfraser i** stedet for tradisjonelle passord. Passordfraser er lengre **kombinasjoner av ord eller setninger** som er lettere å huske, men vanskeligere å knekke. "Icàre@b0utSecur1ty!" er for eksempel en sterk passordfrase.

Tips

Velg først en passordfrase som er lett å huske. Deretter etablerer du ditt eget "krypteringssystem", for eksempel: o=0, i=1, a=@ osv. Pass på at du også integrerer store bokstaver og spesialtegn.

4. Bruk en anerkjent passordadministrator

Bruk en **anerkjent passordadministrator** til å lagre og administrere passordene dine på en sikker måte. Passordadministratorer genererer sterke, unike passord for hver konto og lagrer dem i et kryptert hvelv som kun er tilgjengelig med et hovedpassord.

Tips

Eksempler på anerkjente passordadministratorer finner du i den siste delen av denne læreplanen. Sørg for å bruke passordgenereringsfunksjonen for å få unike, sterke og tilfeldig genererte passord du ikke trenger å huske.

Co-funded by the European Union

4. Beste praksis og gode vaner

4.6. Passordsikkerhet

Sikre passordene dine ved å sørge for at de inneholder følgende elementer.

5. Hold alltid passordene konfidensielle

Del aldri passordene dine med noen, verken venner, familiemedlemmer eller kolleger. Hold passordene dine konfidensielle, og unngå å skrive dem ned eller oppbevare dem på lett tilgjengelige steder. Sørg for å lagre dem i en passordbehandler.

Tips

Hvis det er uunngåelig å dele et passord, er det best å gjøre det muntlig, eller alternativt via en sikker, kryptert applikasjon (f.eks. aldri på sosiale medier). Del aldri påloggingsinformasjon/e-postadresse via samme applikasjon, og gjør det heller via et annet medium.

6. Oppdater passord regelmessig

Oppdater regelmessig passordene dine for nettkontoer, spesielt for sensitive kontoer som bank- og e-postkontoer og kontoer på sosiale medier. Bytt passord umiddelbart hvis du mistenker at de kan ha blitt kompromittert, og la passordadministratoren generere nye passord regelmessig.

Tips

Husk å endre standardpassord som følger med enheter, rutere og programvare. Standardpassord er ofte enkle å gjette seg til og allment kjent, noe som gjør dem sårbare for uautorisert tilgang.

Co-funded by the European Union

SociALL

5. Nyttige verktøy og tilleggsressurser

1. Passordadministratorer
2. 2FA-verktøy
3. Anti-malwares
4. Verktøy for kryptering
5. Andre verktøy

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medicalscan
åpenhet
Co-funded by the European Union

5. Nyttige verktøy og tilleggsressurser

5.1. Passordadministratorer

LastPass 1Password NordPass® KEEPER®

Passordadministratorer **lagrer og administrerer passord på en sikker måte på** tvers av ulike kontoer, noe som forenkler tilgangen samtidig som de sørger for sterke, unike passord og sikker tilgang. Sørg for å:

- **Velge et sterkt, unikt og minneverdig hovedpassord som** gir deg tilgang til passordadministratoren. Pass på at du husker det, og at du aldri gir det videre; det er døren til alle kontoene dine.
- **La passordadministratoren generere sterke, unike passord** for alle kontoene dine. Den husker og lagrer dem, og du vil aldri ha det samme passordet to ganger.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. MPA Medicalscan åpenhet Co-funded by the European Union

5. Nyttige verktøy og tilleggsressurser

5.2. Verktøy for tofaktorautentisering (2FA)

Verktøy for tofaktorautentisering (2FA) øker sikkerheten til en konto ved å tvinge brukeren til å validere påloggingen på to forskjellige, registrerte og pålitelige enheter, vanligvis på telefonen og datamaskinen.

5. Nyttige verktøy og tilleggsressurser

5.3. Anti-malware

Anti-malwares eller anti-virus identifiserer og fjerner ulike typer skadelig programvare og beskytter enheter og nettverk mot cybertrusler i sanntid.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medical Scan
åpenhet
Co-funded by the European Union

5. Nyttige verktøy og tilleggsressurser

5.4. Verktøy for kryptering

Krypteringsverktøy skaper krypterte beholdere som beskytter sensitive filer og mapper ved å hindre uautorisert tilgang gjennom kryptering. Noen verktøy, for eksempel Bitlocker, krypterer eksterne enheter som harddisker for å øke sikkerheten.

Co-funded by the European Union

5. Nyttige verktøy og tilleggsressurser

Navn	Type	Beskrivelse
Privacy Badger	Nettleserutvidelse	Privacy Badger blokkerer sporingskapsler og annonser, og beskytter brukernes personvern ved å hindre tredjepartssporere i å samle inn nettleserdata.
Imprivata	Tilgangsstyring	Imprivata tilbyr enkle sign-on-løsninger som gir helsepersonell sikker tilgang til flere applikasjoner med én pålogging, noe som effektiviserer arbeidsflyten uten at det går på bekostning av sikkerheten.
HIPAA One	Verktøy for samsvar	HIPAA One automatiserer HIPAA-samsvaret og hjelper helseorganisasjoner med å oppfylle myndighetskrav, gjennomføre risikovurderinger og sikre datasikkerhet.
Symantec Endpoint Protection	Sikkerhet for endepunkter	Symantec Endpoint Protection tilbyr omfattende sikkerhet, inkludert avansert trusselbeskyttelse, antivirus og brannmurfunksjoner, som beskytter mot cybertrusler i helsevesenet.
TeamViewer	Tilgang til eksternt skrivebord	TeamViewer gir fjerntilgang til og fjernstyring av enheter, noe som gjør det enklere å få teknisk støtte, utføre feilsøking og samarbeide på tvers av lokasjoner.
Cisco AnyConnect	VPN-verktøy	Cisco AnyConnect tilbyr sikre VPN-tilkoblinger som gir kryptert tilgang til organisasjonsnettverk fra eksterne lokasjoner og beskytter dataoverføringer.
Adobe Sign	Plattform for e-signatur	Adobe Sign legger til rette for sikker digital dokumentsignering, forenkler og fremskynder signeringsprosessen og sørger for samsvar og sikkerhet i dokumenthåndteringen.

Co-funded by the European Union

Takk for din deltakelse og dine ideer!

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
MedicalScar
åpenhet
Co-funded by the European Union