8 TIPS

Du selv enkelt kan gjøre for å redusere risikoen for svindel og dataangrep

verji

Tror du det er de største bedriftene som er mest utsatt for datakriminalitet? Dette stemmer ikke. NHO skriver at i realiteten er mindre bedrifter mer utsatt enn de store, og halvparten av små og mellomstore bedrifter som utsettes for dataangrep, må kaste inn håndkleet innen et halvt år.

De færreste vet at det er e-post som er den største trusselen når vi snakker om datakriminalitet.
Over 90 % av angrepene kommer via e-post, ifølge undersøkelser fra bl. annet Deloitte, A1 Telecom og Verizon. At du vet at e-post er den største trusselen har faktisk en positiv side. Da vet du og din bedrift at det er her dere bør sette inn den største innsatsen.

I dette dokumentet finner du 8 tips til hva dere selv kan gjøre for å redusere risikoen for svindel og dataangrep, for å beskytte dere. Om bedriften din gjør tiltak knyttet til e-posttrusselen, har dere redusert faren for svindel og dataangrep betraktelig. Her er en oversikt over det vi mener er de viktigste tiltakene. Det er ikke nødvendig å gjøre alt på en gang, men lag en plan for å få på plass det dere ikke allerede har på plass, så snart som mulig tilpasset daglig drift.
Når dette er gjennomført har dere «grunnmuren» for datasikkerhet på plass.

---

1. Sørg for at alle ansatte bruker sterke og unike passord
2. Aktiver tofaktor-autentisering (2FA)
3. Oppdater programvare og operativsystemer
4. Bruk antivirusprogram eller endepunktbeskyttelse
5. Sett i verk tiltak for å redusere risikoen for dataangrep og svindel på E-post.
   a. Flytt sensitiv kommunikasjon bort fra e-post
   b. Bruk e-postfiltrering og spam-beskyttelse
6. Bevisstgjør ansatte om phishing og svindel
7. Lag en enkel rutine for verifisering av betalinger
8. Lag en beredskapsplan
9. Veiledninger

1. Sørg for at alle ansatte bruker sterke og unike passord

- Unngå vanlige ord, navn eller tallrekker – bruk lange passord med en blanding av store og små bokstaver, tall og spesialtegn.
- Ikke gjenbruk passord på tvers av systemer.
- Bruk gjerne en passordgenerator, eller dersom du lager passordet selv:
- Bruk en setning inkludert spesialtegn og tall, som for deg er lett å huske, f.eks.: Min2.bil>var() Opel&Rekord. Flett inn stikkord eller ett par bokstaver på systemet du lager passord for. (gjerne mellom parentestegn) På den måten kan du bruke samme setning på flere systemer, men passordet blir allikevel unikt.

2. Aktiver tofaktor-autentisering (2FA)

- Sørg for at alle ansatte aktiverer 2FA på alle systemer dere bruker, i tillegg til sterke og unike passord.

  Vi anbefaler at du bruker en authenticator app, som f.eks. Microsoft Authenticator, Google Authenticator eller Vipps og ikke SMS kode da SMS kode ikke er trygt. Men alle 2FA metoder er bedre enn ingen 2FA.

  2FA er kanskje det viktigste enkelttiltaket en bedrift kan gjøre, så dette bør prioriteres.

  - Office 365 eller andre e-postsystemer
    Se veiledning på side 8.
    Instruksjonsvideo: Overview of multi factor authentication
  - Fagsystemer (trenger du hjelp, kontakt leverandør)
  - Alle SaaS løsninger (trenger du hjelp, kontakt leverandør)

- Ytterligere sikker pålogging – Passnøkler (passkeys)
- Dersom du blir spurt om å ta i bruk Passnøkkell fra en av dine leverandører av system, anbefaler vi at du tar det i bruk.

3. Oppdater programvare og operativsystemer

- Sørg for at alle PC-er og systemer har siste sikkerhetsoppdateringer
- Aktiver automatisk oppdatering der det er mulig, spesielt på Windows, Office programmer og på nettleseren du bruker.
- Slik aktiverer du automatisk oppdatering i Windows:
    - Åpne Innstillinger --> Windows Update
    - Klikk på Avanserte alternativer
    - Sørg for at «Motta oppdateringer automatisk» er aktivert
    - Du kan også aktivere «Oppdater andre Microsoft-produkter samtidig
- Slik aktiverer du automatisk oppdatering på macOS: Skru på “Automatiske oppdateringer” i Systeminnstillinger.
- Aktiver automatisk oppdatering på:
    - Nettlesere
    - PDF lesere og andre apper
    - Mobil OS og apper

4. Bruk antivirusprogram eller endepunktbeskyttelse

- Har virksomheten din eller e-postleverandøren din programmer som filtrerer, stanser og sjekker innholdet i e-postene dine? Dette er noe du bør sørge for. En god start er å ha et godt antivirusprogram eller enda bedre «end point protection» som inkluderer virusprogram, og beskytter alt annet du har på PCen din.
- Dersom dere ikke har noe av dette bør dere umiddelbart ta i bruk Windows Sikkerhet (Windows defender) som er inkludert i Windows, dersom det ikke allerede er gjort.
    - Skriv «Windows sikkerhet» i søkefeltet på oppgavelinjen, åpne Windows sikkerhet og sjekk om det er aktivert. Hvis Windows sikkerhet ikke er aktivert, aktiver det.
    - Sjekk at Virus og trusselbeskyttelse, Kontobeskyttelse, Brannmur og nettverksbeskyttelse, App og nettleserkontroll og Enhetssikkerhet er aktivert. (Under «Hjem» i menyen er det en oversikt)
    - Sjekk at automatisk oppdatering er aktivert. (Finner du under «Virus og trusselbeskyttelse)
    - Skru på Beskyttelse mot løsepengevirus (Finner du under «Virus og trusselbeskyttelse)

5. Sett i verk tiltak for å redusere risikoen for svindel og dataangrep på e-post, som er den største angrepsflaten

Som tidligere nevnt kan over 90% av alle svindelforsøk og dataangrep spores tilbake til e-post. Svindlere og hackere utgir seg ofte for å være en kollega, kunde eller leverandør når de forsøker seg på phishing, ID-tyveri og økonomisk svindel. Ved direktørsvindel og fakturasvindel er avsenders e-post ofte hacket, og det gjør svindelen vanskelig å oppdage – fordi e-postadressen er ekte.

Ved å bruke Verji får du en lukket og kryptert kommunikasjonsplattform der kun verifiserte parter kan delta, og alle meldinger og vedlegg krypteres automatisk. Dette reduserer risikoen dramatiskDette sørger for at all kommunikasjon og fildeling er sikret og i tråd med GDPR, og du har redusert risikoen for svindel og datangrep.

- Flytt e-postkommunikasjon og fildeling internt og med kunder og leverandører til Verji. Ved å bruke Verji får du en lukket og kryptert kommunikasjonsplattform der kun verifiserte parter kan delta, og alle meldinger og vedlegg krypteres automatisk. Dette reduserer risikoen dramatisk.

Automatisk kryptering av filer og meldinger

I Verji blir alle meldinger og vedlegg kryptert automatisk – du trenger ikke tenke på å kryptere og passordbeskytte filer og meldinger, eller annen manuell kryptering. Dette sikrer at sensitive dokumenter som lønn, regnskap, kontrakter og person.

Beskyttelse mot direktørsvindel og fakturasvindel

Ved å bruke Verji til all betalingsrelatert kommunikasjon, hindrer du at svindlere kan utgi seg for ledere eller leverandører via e-post. Verji krever verifisering av brukere og tillater kun kommunikasjon mellom inviterte parter.

GDPR-samsvar uten hodebry

E-post er ikke egnet for behandling av personopplysninger, da e-post ikke er i tråd med GDPR. Verji er utviklet med GDPR i tankene og sørger for at all kommunikasjon skjer i tråd med regelverket – uten at du trenger å gjøre ekstra tiltak.

Enklere samarbeid med kunder og leverandører

Du kan opprette egne rom for hver kunde eller leverandør, og invitere dem inn – helt gratis for dem. Dette gir en trygg og profesjonell kanal for dialog, dokumentdeling og signering.

Dersom dere ikke allerede bruker Verji, kan dere prøve Verji gratis og uforpliktende ved å gå til vår nettside. Start fri prøveperiode - Verji

Eller kontakte oss på:

- E-post: sales@verji.com
- Telefon: 90 53 24 54

Andre tiltak du bør overveie og iverksette:

- Husk å få på plass to-faktor autentisering.
- Bruk e-postfiltrering og SPAM beskyttelse. De fleste e-postleverandører tilbyr innebygde filtre mot phishing og spam. Sørg for at disse er aktivert og oppdatert. Se veiledning side 7
- Bevisstgjør ansatte om phishing og svindel.

(Se punkt 6. Opplæring og bevisstgjøring av ansatte)

6. Opplæring og bevisstgjøring av ansatte

Bevisstgjør ansatte om phishing og svindel. Hva du bør være obs på i e-poster:

Uvanlige avsendere eller e-postadresser

Sjekk alltid e-postadressen nøye – svindlere bruker ofte adresser som ligner på ekte, men har små avvik (f.eks. support@micros0ft.com).

Vær ekstra skeptisk hvis du får e-post fra noen du ikke har hatt kontakt med før.

Språk og tone

- Dårlig grammatikk, oversettelser eller uvanlig formell/uformell tone kan være tegn på svindel.
- E-poster som skaper hastverk eller frykt (“Svar innen 10 minutter!”) er typiske phishing-triks.

Uventede forespørsler om:

- Informasjon (BankID, passord, fødselsnummer m.m)
- Penger, overføring av penger, betaling av faktura.
- Endring av kontonummer på betalinger, faktura etc.

Lenker og vedlegg

- Hold musen over lenker før du klikker – sjekk om adressen ser ekte ut.
- Ikke åpne vedlegg du ikke forventer, spesielt ZIP-filer, .exe eller makroaktiverte dokumenter.

E-poster som utgir seg for å være fra kjente tjenester

- Svindlere utgir seg ofte for å være fra Microsoft, banken, Altinn, Posten osv. Sjekk alltid om du kan logge inn direkte på tjenesten via nettleseren – ikke via lenken i e-posten.
- Sørg for at alle ansatte leser Norsis sine råd og veiledninger: E-post - NorSIS

7. Opplæring og bevisstgjøring av ansatte

- Bruk Verji til all betalingsrelatert kommunikasjon dersom dere har Verji. Dersom dere ikke har Verji:
- Ikke aksepter en enkel henvendelse via e-post, SMS, eller telefon.
- Bli enige om hvilke alternative bekreftelser som skal gjøres.

8. Lag en beredskapsplan og søk hjelp når det er behov.

- Lag en enkel beredskapsplan for hva som må gjøres dersom dere blir utsatt for databrudd
- Avklar hvem dere kan kontakte for å få hjelp, inngå gjerne en avtale med en sikkerhetspartner.
- Tegn gjerne en Cyberforsikring, de fleste tilbyr hjelp ved en hendelse.
- Se utkast til enkel plan på side 9 og 10.

Prøve Verji gratis og uforpliktende: Start fri prøveperiode - Verji

9. Veiledninger

Slik aktiverer du selv 2FA i Office 365 (Microsoft 365)

- Logg inn på Microsoft 365 Admin Center
- Gå til: https://admin.microsoft.com
- Gå til “Brukere” “Aktive brukere”
- Her ser du en liste over alle brukere i organisasjonen.
- Klikk på “Multifaktorautentisering”
- Du finner dette under “Flere innstillinger” eller via en egen lenke nederst.
- Velg brukeren du vil aktivere 2FA for
- Huk av ved siden av navnet.
- Klikk “Aktiver”
- Bekreft at du vil aktivere tofaktorautentisering.
- Brukeren må fullføre oppsettet ved neste innlogging
- De vil bli bedt om å legge til en ekstra metode – f.eks. mobilapp, SMS eller telefon.
- Leveres Office 365 av en leverandør, kan du be leverandøren ordne dette

Slik aktiverer og justerer du e-postfiltrering og spam-beskyttelse i Office 365.

1. Logg inn i Microsoft 365 Admin Center
- Gå til: https://admin.microsoft.com
- Logg inn med en administratorkonto.

2. Gå til Exchange Admin Center (EAC)
- I venstremenyen, klikk på “Admin centers” “Exchange”.
- Du kommer til Exchange Admin Center (EAC).

3. Naviger til “Protection” “Spam filter”
- Her finner du eksisterende spamfilter-policyer.
- Du kan redigere standardpolicyen eller opprette en ny.

4. Rediger eller opprett en policy
- Klikk på policyen “Edit”.

Her kan du:

- Justere terskelen for spam (lav, middels, høy).
- Aktivere karantene for mistenkelige meldinger.
- Velge hva som skal skje med spam (leveres til søppelpost, karantene, slettes).
- Aktivere SPF, DKIM og DMARC-beskyttelse (anbefales).

5. Bruk Outlook-klienten

- Outlook har også lokal spamfiltrering:
- Gå til "Hjem"-fanen "Søppelpost" "Søppelpostalternativer".
- Velg ønsket beskyttelsesnivå (lav, høy, kun sikre lister).
- Du kan også legge til avsendere i "Sikre avsendere"-listen.

10. Enkel beredskapsplan

Formål

- Sikre rask og effektiv håndtering ved mistanke om eller bekreftet databrudd, for å begrense skade, gjenopprette drift og oppfylle lovpålagte krav.

Opprette hendelsesresponsteam

- Utnevn et team av personer med ulike roller og ansvarsområder som skal være ansvarlige for å reagere på cybersikkerhetshendelser.
  De bør være minimum 2 personer og disse må være kjent for øvrige ansatte

Varsling og første tiltak

Den som oppdager eller mistenker et databrudd skal umiddelbart varsle:

- [Navn på ansvarlig person] – IT-ansvarlig / daglig leder
- Hendelsesresponsteam

Første tiltak:

- Informer ansatte om å ikke starte sin PC.
- Koble berørte enheter fra internett og interne nettverk
- Ikke slett eller endre filer – bevar spor
- Noter tidspunkt, hva som ble oppdaget og hvilke systemer som er berørt

Kontakt forsikringsselskap og/ eller sikkerhetspartner

- Samhandle med disse

Ansvarlig person/ hendelsesresponsteam skal:

- Bekrefte om det foreligger et faktisk brudd
- Vurdere om personopplysninger er berørt
- Vurdere om drift, kunder eller økonomi er påvirket

Begrensning og sikring

- Isoler berørte systemer og brukere
- Endre passord og tilgangsnøkler
- Steng eventuelle eksterne tilganger midlertidig
- Informer ansatte om tiltak og videre prosess

Varsling til eksterne

Ved brudd på personopplysninger:

- Meld til Datatilsynet innen 72 timer: https://www.datatilsynet.no
- Vurder om berørte personer/ kunder skal varsles

Ved alvorlig hendelse:

- Vurder å kontakte politiet / Økokrim