

#1

Du bliver bedt om at overføre penge, betale en faktura eller ændre betalingsoplysninger

Kan være tegn på: Forsøg på økonomisk svindel

REAGÉR HVIS

- En faktura er uventet.
- En afsender oplyser om ændrede kontooplysninger.
- Du bliver bedt om at ændre en medarbejders lønkonto.
- Der gives en meget kort betalingsfrist, eller fristen er overskredet.
- Et beløb skal overføres til en ny eller udenlandsk konto.
- En anmodning lægger pres på dig.
- Din chef anmoder uventet om en betaling eller et indkøb.
- Du bliver anmodet om at købe gavekort.

DET SKAL DU GØRE

STRAKS

STOP

Gennemfør **ikke** betalingen.

Videresend **ikke** den mistænkelige mail eller henvendelse.

BEKRÆFT OG ORIENTÉR

Be- eller afkræft, om fakturaen er falsk, ved at kontakte afsenderen på et kendt telefonnummer eller søg deres hovednummer frem. Brug **ikke** telefonnummer eller kontaktoplysninger fra henvendelsen.

Orientér din leder og få bekræftet anmodningen internt i virksomheden, før der overføres penge.

Gør dine kollegaer opmærksomme på henvendelsen mundtligt eller ved skærbilleder.

AFSLUTTENDE

- Gør alle i virksomheden opmærksom på hændelsen mundtligt eller ved skærbilleder.
- Brug virksomhedens funktion til rapportering af phishing, hvis den findes. Slet først beskeden, når den er blevet håndteret efter virksomhedens procedure.
- Udarbejd eller gennemgå procedure for pengeoverførsler.



#2

Du har betalt en faktura, overført penge eller ændret betalingsoplysninger

Kan være tegn på: Økonomisk svindel – med gennemført pengeoverførsel

REAGÉR HVIS

- Der er usædvanlig aktivitet på virksomhedens bankkonti.
- Fakturaen var uventet.
- Afsenderen oplyste om ændrede kontooplysninger.
- Der var en meget kort betalingsfrist, eller fristen var overskredet.
- Beløbet er overført til en udenlandsk konto.
- Anmodningen lagde pres på dig.

STRAKS

STOP

Undlad at godkende flere fakturaer, overførsler eller ændringer i betalingsoplysninger, før sagen er undersøgt.

Ring straks til banken på et kendt akutnummer. Hav beløb, tidspunkt, modtagerkonto og transaktions-id klar.

BEKRÆFT

Sæt virksomhedens økonomiansvarlige og din nærmeste leder ind i sagen.

Be- eller afkræft, om fakturaen er falsk, ved at kontakte afsenderen på et kendt telefonnummer eller søg deres hovednummer frem. Brug **ikke** telefonnummer eller kontaktoplysninger fra henvendelsen.

DET SKAL DU GØRE

AFSLUTTENDE

SIKR BEVISER OG ANMELD

- Bevar original mail eller besked, faktura, kontonummer, beløb, tidspunkt, transaktions-id, bankkvittering, relevante kontaktoplysninger og en kort tidslinje.
- Anmeld hændelsen til politiet, datatilsynet og forsikringen, hvis det er relevant.

KOMMUNIKÉR

- Gør alle i virksomheden opmærksomme på hændelsen mundtligt eller ved skærbilleder. Videre send **ikke** henvendelsen.
- Brug virksomhedens funktion til rapportering af phishing, hvis den findes. Slet først beskeden, når den er blevet håndteret efter virksomhedens procedure.
- Udarbejd eller gennemgå procedure for pengeoverførsler.



#3

Du bemærker usædvanlig aktivitet i dit mailprogram

Kan være tegn på: Hacking af virksomhedens eller medarbejderens mailkonto

REAGÉR HVIS

- Der er sendt en mail fra din konto, men du kan ikke se den i mappen "sendt post" eller genkende at have sendt mailen.
- Der registreres login fra ukendte enheder, steder, tidspunkter mv.
- Der er opsat automatisk videresendelse eller andre ukendte indbakke-/mailregler.
- Din mailkonto er låst eller din kode pludselig er ændret.

DET SKAL DU GØRE

STRAKS

STOP OG ORIENTÉR

- Stop med at bruge mailkontoen, indtil hændelsen er håndteret.
- Orientér din leder og kontakt straks jeres it-ansvarlige eller it-leverandør fra en anden enhed f.eks. telefon.
- Gør dine kollegaer opmærksomme på mistanken.

UNDERSØG

- Tjek, om der er ændret i mailkontoens regler eller indstillinger, fx automatisk videresendelse, sletning eller flytning af mails.
- Tag skærbilleder af alt, der ser usædvanligt ud. De skal bruges, hvis hændelsen skal anmeldes.

AFSLUTTENDE

HVIS DET ER BEKRÆFTET, AT JERES KONTI ER HACKET

Advar og anmeld

- Anmeld hændelsen til politiet, datatilsynet, forsikringen og banken, hvis det er relevant.
- Overvej at kontakte jeres kunder, samarbejdspartnere og leverandører via en sikker kanal (f.eks. opkald) og gør dem opmærksomme på, at I har været hacket. De skal derfor være varsomme ved henvendelser, de har modtaget fra jer.
- Vær særlig opmærksom på forsøg på svindel i denne kommende periode.



#4

Du bliver bedt om at afgive oplysninger om dig selv eller virksomheden

Kan være tegn på: Forsøg på digital svindel

REAGÉR HVIS

- Den pågældende mail, SMS eller opkald er uventet og mistænkelig.
- Du ikke kan genkende mailadressen eller telefonnummeret.

Du bliver bedt om at:

- Reagere hurtigt.
- Klikke på et link.
- Afgive loginoplysninger, kode eller andre sensitive oplysninger.

STRAKS

STOP

- Klik ikke på linket.
- Svar ikke på beskeden.
- Indtast ikke MitID, loginoplysninger mv.
- Videre send **ikke** mailen til andre.

BEKRÆFT

- Del din mistanke med en kollega mundtligt eller telefonisk. Del evt. skærbilleder af mailen.
- Ring til afsenderen for at få mailen bekræftet. Ring på et hovednummer eller det telefonnummer, du plejer at bruge. Brug **ikke** telefonnummer eller kontaktoplysninger fra henvendelsen.

Hvis du har klikket på et link og afgivet oplysninger

- Gå til actioncard #5.

DET SKAL DU GØRE

AFSLUTTENDE

- Gør alle i virksomheden opmærksom på hændelsen mundtligt eller ved skærbilleder. Videre send **ikke** mailen.
- Brug virksomhedens funktion til rapportering af phishing, hvis den findes.
- Slet først beskeden, når den er blevet håndteret efter virksomhedens procedure.



#5

Du har afgivet oplysninger om dig selv eller virksomheden

Kan være tegn på: I er udsat for digital svindel

REAGÉR HVIS

- Den pågældende mail, SMS eller opkald er uventet og mistænkelig.
- Du ikke kan genkende mailadressen eller telefonnummeret.
- Du har indtastet sensitive oplysninger såsom MitID, loginoplysninger mv.

Du blev bedt om at:

- Reagere hurtigt.
- Klikke på et link.
- Afgive sensitive oplysninger.

STRAKS

STOP

Stop handlingen og tag skærbilleder af alt, der ser mistænkeligt ud f.eks. den hjemmeside, du har indtastet oplysningerne på.

Hvis du har brugt MitID eller MitID Erhverv i forbindelse med hændelsen, skal du straks kontakte Cyberhotline for digital sikkerhed på **+45 33 37 00 37**.

Ring til banken og sæt dem ind i situationen.

Orientér din leder, it-ansvarlige eller it-leverandør.

BEGRÆNS

Hvis du har afgivet loginoplysninger:

- Ændr dine adgangskoder og hvis muligt, opsæt flerfaktorgodkendelse efter aftale med den it-ansvarlige.

Gør alle i virksomheden opmærksom på hændelsen mundtligt eller ved skærbilleder. Videre send **ikke** henvendelsen.

DET SKAL DU GØRE

AFSLUTTENDE

Advar og anmeld

- Anmeld hændelsen til politiet, datatilsynet og forsikringen, hvis relevant.
- Brug virksomhedens funktion til rapportering af phishing, hvis den findes.
- Slet først beskeden, når den er blevet håndteret efter virksomhedens procedure.
- Vær særlig opmærksom på forsøg på svindel i denne kommende periode.