SVINDELVAGT · DANMARK · SMÅ VIRKSOMHEDER · UGENTLIG UDGAVE · 24. november 2026

Svindel og sikkerhedsvarsler for din virksomhed

En letlæst guide for små danske virksomheder — den svindel, der tømmer konti, og de sårbarheder, hackere udnytter lige nu.

Udgivet af: **lennartandersen.xyz**

Hvis I tror, I lige er blevet ramt

1. **Ring straks til jeres bank.** En overførsel kan nogle gange kaldes tilbage — men kun inden for få timer.
2. **Svar ikke på mailen.** Ring til personen eller leverandøren på et nummer, I havde i forvejen.
3. **Afbryd, slet ikke.** Tag den ramte computer af netværket, men lad den være tændt — beviser hjælper med genopretning og forsikring.

Hvem I skal kontakte i Danmark

ANMELD DET

Politiet

114

Anmeld svindel mod virksomheden — også forsøg. Kan ofte anmeldes digitalt på politi.dk. Forsikring og bank skal typisk bruge journalnummeret.

FÅ HJÆLP

Cyberhotline for digital sikkerhed

33 37 00 37

For borgere og virksomheder: råd og henvisning ved svindel og cyberangreb. Hverdage 8–20, weekend og helligdage 10–16.

RING NU

Jeres banks erhvervsservice

Nummeret på kortet

Første opkald efter enhver mistænkelig betaling. Bed om tilbagekaldelse og spærring. Kort: Nets 44 89 29 29 (døgnet rundt).

HOLD JER OPDATERET

Styrelsen for Samfundssikkerhed

samsik.dk

Den nationale myndighed for cybersikkerhed. Trusselsvurderinger, varsler og råd til små virksomheder.

Seks regler, der stopper det meste svindel

- **Bekræft alle ændringer af bankoplysninger pr. telefon.** Ny konto hos en leverandør? Ring på det nummer, I havde i forvejen — aldrig det i mailen.
- **To personer godkender betalinger.** Nye modtagere eller store overførsler kræver en anden persons godkendelse. Ingen undtagelser for »hastesager«.
- **Slå totrinsbekræftelse til** på mail, netbank, løn og regnskab. En hacket mailkonto står bag det meste virksomhedssvindel.
- **Opdater software, der vender mod internettet, inden for dage,** ikke måneder — hjemmeside, VPN, firewall, mailserver. Se live-listen på næste side.
- **Hav offline-backup, og test den.** Rammer ransomware, er en testet backup forskellen på en dårlig dag og at lukke.
- **Ingen betaler med gavekort.** En »chef«, der skriver til en medarbejder om at købe gavekort til en kunde, er svindel — hver gang.

Nummeret på din skærm kan være falsk

Svindlere kan vise et hvilket som helst nummer — selv det rigtige nummer til din bank, politiet eller Skattestyrelsen. Det kaldes **spoofing**. Beder et opkald om penge, koder, MitID-godkendelse eller personlige oplysninger, så **læg på og ring selv op** på nummeret bag på dit kort eller fra den officielle hjemmeside.

Bloker svindelopkald på din egen telefon

- **Android:** Telefon-appen → Indstillinger → *Opkalds-id og spam* → slå spamfiltrering til (Samsung: *Opkalds-id og spambeskyttelse*). Pixel har også *Opkaldsscreening*.
- **iPhone:** Indstillinger → Telefon (eller Apps → Telefon) → *Gør ukendte opkald lydløse*: numre uden for dine kontakter går til telefonsvareren.
- **Enkelte numre:** bloker dem fra seneste opkald — det hjælper lidt, men svindlerne skifter nummer hele tiden.
- **Dit teleselskab:** mange tilbyder gratis filtrering af spamopkald — spørg dem.

Opdater nu — sårbarheder, hackere udnytter denne måned

Tilføjet inden for de sidste 30 dage til den amerikanske myndighed CISA's liste over kendte udnyttede sårbarheder (cisa.gov/kev) — hackere bruger dem aktivt. Kører jeres virksomhed, webhotel eller it-leverandør noget af dette, så opdater nu. Data pr. 24. november 2026.

Software	Sårbarheds-ID	Markeret
Broadcom VMware vCenter	CVE-2026-123890	2026-11-20
Cisco Expressway Series	CVE-2026-76466	2026-11-20
Synology DiskStation Manager (DSM) RANSOMWARE	CVE-2024-10441	2026-11-18
Microsoft Office	CVE-2026-124194	2026-11-10
Cisco BroadWorks	CVE-2026-20320	2026-11-10
Barracuda Networks Multiple Products	CVE-2026-111560	2026-11-10
Barracuda Email Security Gateway (ESG)	CVE-2026-116606	2026-11-10
Google Chromium	CVE-2026-125350	2026-11-10
SonicWall SonicOS SSLVPN	CVE-2026-19868	2026-11-06
Apple Multiple Products	CVE-2024-27834	2026-11-04
WordPress Core	CVE-2026-119977	2026-11-03
Ivanti Connect Secure	CVE-2026-118527, CVE-2026-111357	2026-10-30
Secure Firewall ASA Software and Cisco Secure FTD Software	CVE-2026-76418	2026-10-29
Broadcom VMware ESX	CVE-2026-41709	2026-10-28
Adobe Commerce and Magento	CVE-2026-48356	2026-10-27

Har I ikke selv servere? Send denne side til jeres webhotel eller it-leverandør og spørg: »Er vi berørt, og er det opdateret?«

Seneste fra Styrelsen for Samfundssikkerhed

- 2026-11-24 — **Ny brancheaftale med mobilselskaber om prioritering i krisesituationer**
- 2026-11-24 — **Børn, unge og socialt udsatte skal lære om beredskab og krisesituationer**
- 2026-11-23 — **Nye nationale råd til borgere mod digital svindel**
- 2026-11-20 — **5,6 millioner til innovative projekter i ny cybersikkerhedschallenge**
- 2026-11-18 — **Styrelsen for Samfundssikkerhed gør opmærksom på nye Java-sårbarheder**
- 2026-11-17 — **Kvantecomputere kan true Danmarks cybersikkerhed – nu lanceres nyt projekt til hjælp for virksomheder og myndigheder**
- 2026-11-06 — **Virksomheder bør styrke deres cyberforsvar**
- 2026-11-05 — **Styrelsen for Samfundssikkerhed er opmærksom på, at pro-russiske hackergrupper tager ansvar for cyberangreb**
- 2026-11-04 — **Beskyt jeres tekniske systemer mod cyberangreb**
- 2026-11-02 — **Styrelsen for Samfundssikkerhed følger sagen om cyberangreb mod køle- og frysesystemer i Europa**

Alle nyheder og varsler: samsik.dk.

Linux-servere — kritiske fejl, hackere udnytter

De 10 sårbarheder i Linux-kernen og Linux-distributioner, der senest er tilføjet til CISA's liste. De fleste hjemmesider, cloudservere, VPS'er og NAS-bokse kører Linux. Rettelser til kernen virker først efter en **genstart** — spørg jeres webhotel eller it-leverandør: »Er kernen opdateret, og er serveren genstartet?«

Software	CVE	Markeret	Software	CVE	Markeret
OpenBSD OpenSSH	CVE-2026-123158	2026-11-09	**Linux Kernel**	CVE-2026-53362	2026-08-27
Linux Kernel	CVE-2026-46300	2026-10-28	**Red Hat Libuser**	CVE-2015-3246	2026-08-26
Linux Kernel	CVE-2025-39964	2026-09-18	**Red Hat Automatic Bug Reporting Tool**	CVE-2015-5287	2026-08-26
Linux Kernel	CVE-2026-53266	2026-09-18	**Linux Kernel**	CVE-2022-0995	2026-08-26
Linux Kernel	CVE-2025-39682	2026-09-18	**Linux Kernel**	CVE-2022-0492	2026-06-02

Den svindel, der rammer danske virksomheder

Leverandørmail med »nye bankoplysninger«

En mail fra en rigtig leverandør — eller en næsten identisk adresse — siger, at kontonummeret er ændret, og at næste faktura skal betales til en ny konto. Ofte sendt fra en ægte, hacket mailkonto.

> **Afsløringen:** Enhver ændring af betalingsoplysninger pr. mail. Ring til leverandøren på et kendt nummer, før I betaler.

Direktørsvindel (CEO-fraud)

En besked »fra direktøren« — nogle gange en klonet stemme i telefonen — beder bogholderiet om en hastende, fortrolig betaling eller om at købe gavekort til en kunde.

> **Afsløringen:** Hemmelighed, hast og »jeg kan ikke tale lige nu«. Bekræft ansigt til ansigt eller ved at ringe tilbage.

Ransomware fra ét klik

En medarbejder åbner en falsk faktura, et forsendelsesvarsel eller et delt dokument. Dage senere er alle filer krypteret, og et krav om løsesum dukker op.

> **Afsløringen:** Uventede vedhæftninger og »log ind for at se dokumentet«-sider. Meld det, klik ikke.

Falsk henvendelse fra Skattestyrelsen

En mail eller et opkald siger, at jeres moms er i restance, at CVR-nummeret bliver lukket, eller at der er penge til gode — betal eller log ind via et link i dag.

> **Afsløringen:** Skattestyrelsen beder aldrig om betaling via link, gavekort eller krypto. Log selv ind på skat.dk via MitID Erhverv.

Falske fakturaer og registre

Regninger for fornyelse af domæne, »varemærkeregistre«, opslag i brancheregistre eller kontorartikler, I aldrig har bestilt — i håb om, at nogen i bogholderiet bare betaler.

> **Afsløringen:** En leverandør, I aldrig har brugt, eller småt, der siger, at I har »accepteret« i telefonen.

Falsk it-support og »jeres konto er låst«

Et opkald eller en pop-up udgiver sig for at være Microsoft eller jeres it-leverandør og beder en medarbejder installere fjernadgang eller godkende et login.

> **Afsløringen:** En uventet godkendelsesanmodning på telefonen. Har du ikke lige logget ind, så afvis og sig det til it.

Dette er generel information og ikke juridisk, økonomisk eller politimæssig rådgivning. Telefonnumrene er tjekket på organisationernes egne hjemmesider (senest tjekket november 2026), men numre og procedurer ændrer sig — bekræft altid et nummer på den officielle hjemmeside, før du stoler på det. Ring altid 112 i en nødsituation. Live-afsnittene er dannet automatisk den 24. november 2026 ud fra CISA's KEV-katalog og Styrelsen for Samfundssikkerheds nyhedsfeed; de er ikke en vurdering af jeres systemer.