ITAGIL
WE MAKE IT EASY

WEBINAR · 24. SEPTEMBER 2026

Awareness & Phishing

Forstå truslerne før de rammer

Er I klar til de nye cybertrusler?

DAGENS VÆRT

Andreas Hertz Jensen

IT-konsulent, Awareness & Phishing Specialist, ITAGIL

Dagsorden

01 Phishing i mange former

02 Adgangskoder og MFA

03 En personlig historie

04 Hvad kan man så gøre?

05 Cases fra den store verden

06 Sådan spotter du et falsk link

ITAGIL
WE MAKE IT EASY

01

Phishing i mange former

01 · PHISHING I MANGE FORMER

Et bredt trusselsbillede

Mail og beskeder

Phishing

Spear phishing

Whaling

CEO-svindel

Smishing (SMS)

Quishing (QR)

Telefon og stemme

Vishing

Deepfake-stemmer

Callback-phishing

Falsk it-support

MFA-træthed

Web og links

Drive-by URLs

Falske login-sider

Typosquatting

Malvertising

Pharming

Adversary-in-the-middle

Social Engineering

Pig butchering

Romance scams

Falske profiler

Falske jobtilbud

Angler phishing

Skadelig software

Malware

Trojan horse

Ransomware

Infostealers

Keyloggers

Spyware

ITAGIL
WE MAKE IT EASY

02

Adgangskoder og MFA

Gode og dårlige adgangskoder

✕ Dårlig

Sommer2026!

Firmanavn123

Fido1987

Korte, forudsigelige og ofte genbrugt på tværs af tjenester.

✓ God

Kaffe-Regnvejr-Cykel-Tønder

27 tegn · nem at huske · svær at gætte

En unik adgangskode til hver tjeneste

Gemt i en password manager

Altid kombineret med MFA

Tid til at knække en adgangskode

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	46 mins	2 hours	3 hours
6	Instantly	37 mins	2 days	5 days	1 week
7	Instantly	16 hours	3 months	10 months	2 years
8	Instantly	2 weeks	12 years	50 years	132 years
9	2 hours	1 year	636 years	3k years	9k years
10	20 hours	32 years	33k years	191k years	645k years
11	1 week	839 years	1m years	11m years	45m years
12	3 months	21k years	89m years	737m years	3bn years
13	2 years	567k years	4bn years	45bn years	221bn years
14	23 years	14m years	241bn years	2tn years	15tn years
15	229 years	383m years	12tn years	175tn years	1qd years
16	2k years	9bn years	653tn years	10qd years	75qd years
17	22k years	259bn years	33qd years	675qd years	5qn years
18	228k years	6tn years	1qn years	41qn years	372qn years

Hive Systems

Hvert ekstra tegn gør et brute force-angreb markant langsommere.

Længde betyder mere end specialtegn.

Kilde: Hive Systems

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	Instantly
9	Instantly	Instantly	Instantly	Instantly	Instantly
10	Instantly	Instantly	Instantly	Instantly	Instantly
11	Instantly	Instantly	Instantly	Instantly	Instantly
12	Instantly	Instantly	Instantly	Instantly	Instantly
13	Instantly	Instantly	Instantly	Instantly	Instantly
14	Instantly	Instantly	Instantly	Instantly	Instantly
15	Instantly	Instantly	Instantly	Instantly	Instantly
16	Instantly	Instantly	Instantly	Instantly	Instantly
17	Instantly	Instantly	Instantly	Instantly	Instantly
18	Instantly	Instantly	Instantly	Instantly	Instantly

OK, hvis du nu skulle spørge for en ven:

Hvad hvis min kode er blevet ståjet før, bruger almindelige ord fra ordbogen eller er blevet genbrugt?

Så er det desværre en anden sag.

Kilde: Hive Systems

Multifaktor-godkendelse

FAKTOR 1

Noget du ved

Adgangskode, PIN-kode

FAKTOR 2

Noget du har

Telefon med app, sikkerhedsnøgle

FAKTOR 3

Noget du er

Fingeraftryk, ansigtsgenkendelse

PAS PÅ MFA-TRÆTHED Godkend aldrig en login-anmodning, du ikke selv har startet.

04

Hvad kan man så gøre?

Et stærkere menneskeligt forsvar

01

Simuleret phishing

Realistiske testmails, der tester på alle følelser som frygt, grådgihed, og nysgerrighed

02

Kort træning

Små læringsmoduler der maks tager 5 min.

03

Måling

Klar rapportering på, hvor I står, og hvordan I udvikler jer

04

Løbende

Awareness er en vane, ikke et kursus. Vi holder den ved lige.

Det kræver kun ét forkert klik

1

Ét klik

En medarbejder åbner et link i en troværdig mail

2

Stjålet login

Brugernavn og adgangskode indtastes på en falsk side

3

Adgang

Angriberen logger ind på mail, filer og systemer

4

Spredning

Nye mails sendes fra en ægte konto til kolleger og kunder

5

Konsekvens

Ransomware, svindel, datalæk og nedetid

05

Cases fra den store verden

MGM Resorts, 2023

Et telefonopkald til it-helpdesken, hvor angriberen udgav sig for at være en medarbejder, blev starten på et af årets største angreb.

How the MGM Cyber Attack Unfolded

Social Engineering Tactics Used by Hackers

To gain access to the MGM network, Scattered Spider launched a vishing social engineering attack that went something like this:

1. Scattered Spider members researched MGM employees on LinkedIn, gathering information about their roles and identities.
2. Using the gathered information, the attackers chose an MGM employee to impersonate.
3. The hackers called MGM's IT help desk, posing as the employee and successfully convinced the help desk into providing them with login credentials.
4. Using the obtained credentials, Scattered Spider gained administrator privileges to MGM's Okta and Azure tenant environments.
5. The attackers used their high-level access to move laterally within MGM's systems.

~100 mio. $

MGM's eget estimat af tabet

Arup, 2024

Et videomøde med økonomidirektøren og flere kolleger – hvor alle deltagere var AI-genererede deepfakes.

Mail	Besked om en fortrolig transaktion *Fra britisk økonomidirektør til finansafdeling I HongKong
Tvivl	Medarbejderen var i første omgang skeptisk
Deepfake	Videomødet med "kollegerne" fjernede tvivlen
Opdaget	Først ved kontakt til hovedkontoret

~25 mio. $

Overført i 15 transaktioner

ITAGIL
WE MAKE IT EASY

06

Sådan spotter du et falsk link

Anatomien af et link

https://	login.microsoft.com.	secure-verify.net	/reset
Protokol	Subdomæner – kan være hvad som helst	Det rigtige domæne	Sti

➔ Find den første **/** efter https:// og læs baglæns. De to sidste led før skråstregen er domænet.

Altid hold øje med det rigtige domæne.

Domæner og subdomæner

login.microsoft.com	✓	Subdomæne af microsoft.com
microsoft.com.login-help.net	✗	Domænet er login-help.net
rnicrosoft.com	✗	"rn" ligner et "m"
mitid.dk	✓	Det officielle domæne
mitid-dk.com	✗	Et helt andet domæne
postnord-levering.info	✗	Kendt navn på et fremmed domæne

Fem hurtige tjek

1	**Hold musen over linket**	Se den rigtige adresse, før du klikker
2	**Tjek afsenderens domæne**	Navnet kan forfalskes – adressen afslører mere
3	**Stop op ved hast og pres**	"Inden for 24 timer" er et klassisk tegn
4	**Vær skeptisk over for QR-koder**	De skjuler adressen, indtil det er for sent
5	**Ring op på et kendt nummer**	Aldrig nummeret i den mistænkelige besked

Tak for i dag

Prøv awareness- og phishingtræning gratis i 2 uger

KONTAKT

Andreas Hertz Jensen

IT-konsulent, ITAGIL

ahje@itagil.dk