IT Security
Arne Hagesæther

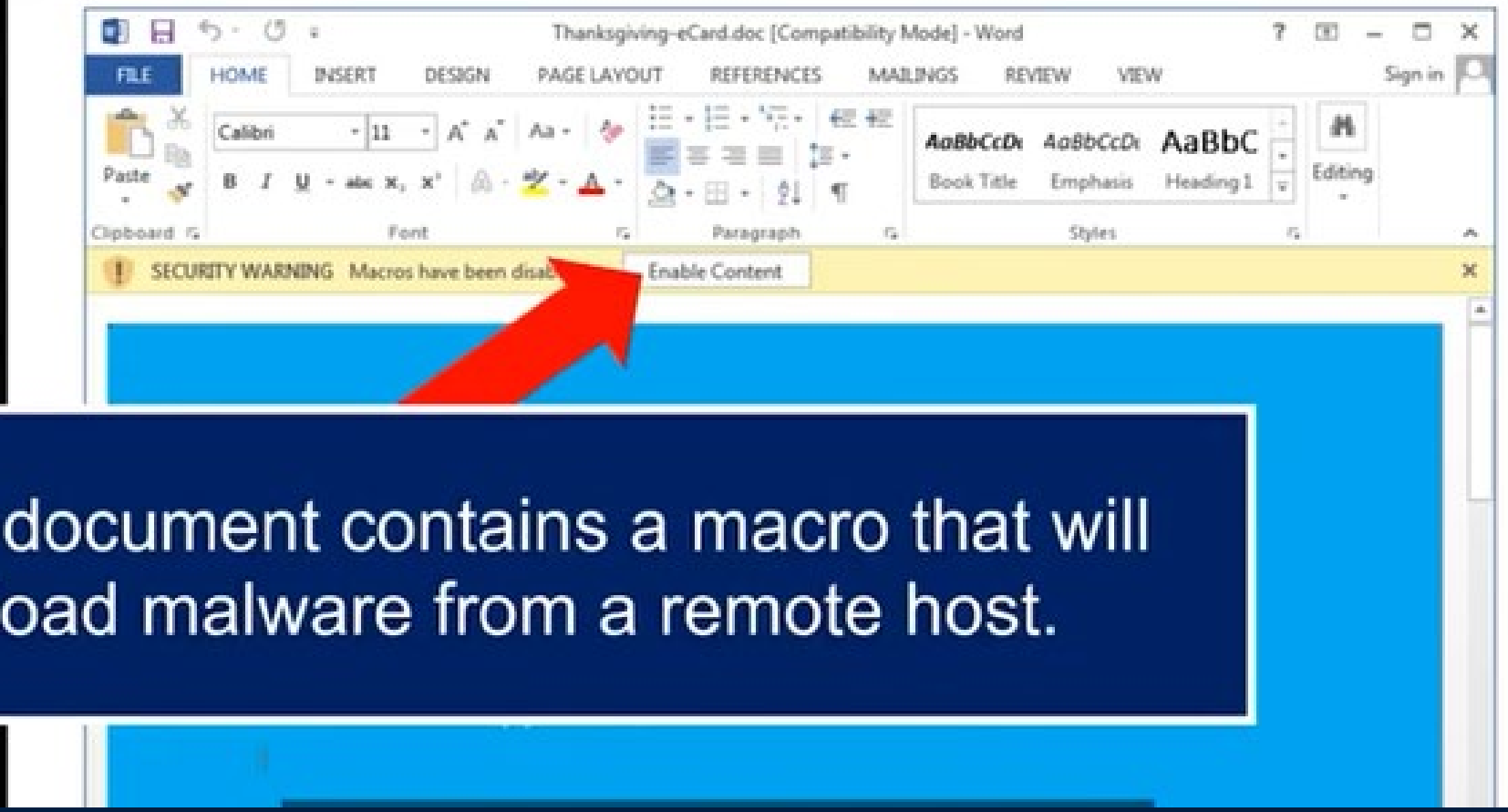
The past

In 2020 ScaleAQ got hit by a ransomware attack that cost the company millions.

The Attack


Remote Platform Hacking
Email Phishing Schemes
Compromised Employee Credentials

1. The Attack

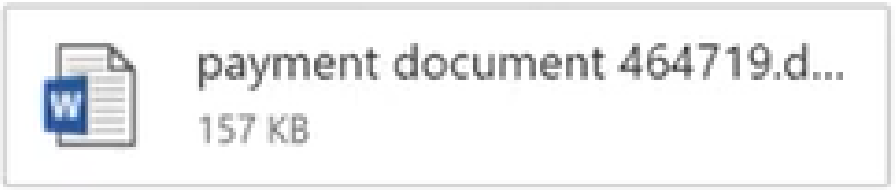


Word document contains a macro that will download malware from a remote host.

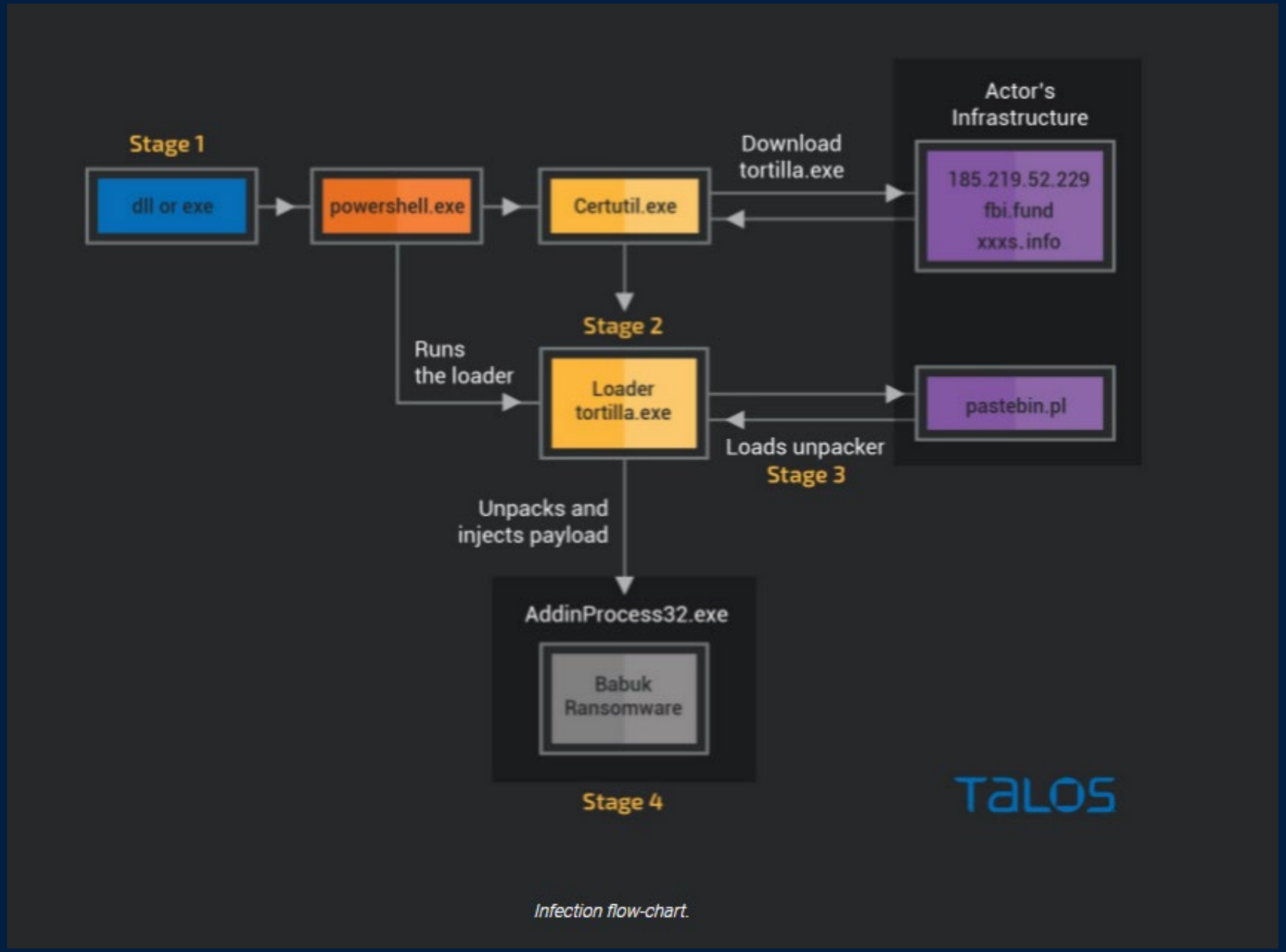
John Hawkins Inbox

John.Hawkins@globo.com
to me

Your contact details (johnsmith@gmail.com) was specified as the destination of the payment. The funds will be posted within 5 hours.
The password is 0fghy521. You have to type this to be able to view the document.




resume
JL
Jeff Lanza
Today, 7:52 AM
Jeff Lanza
Reply all
https://www.dropbox.com/s/mtorrewyka41l7o/resume.pdf?dl=0
resume.pdf
www.dropbox.com
Shared with Dropbox



Infection flow-chart.

2. The Encryption

3. The Notification

What happened to your files?
All your files are encrypted with RSA-4096, Read more on
https://en.wikipedia.org/wiki/RSA_(cryptosystem)
RSA is an algorithm used by modern computers to encrypt and decrypt the data. RSA is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone:

4. The Demand

OPTION 1
Step 1 : You must send us 3 Bitcoin(s) for each affected system
Step 2 : Inform us in panel with hostname(s) of the system you want, wait for confirmation and get your decrypter
OPTION 2
Step 1 : You must send us 13 Bitcoin(s) for all affected system
Step 2 : Inform us in panel, wait for confirmation and get all your decrypters

Our Bitcoin address is: xxx

BE CAREFUL, THE COST OF YOUR PAYMENT INCREASES $10,000 EACH DAY AFTER THE FOURTH DAY

5. Don’t try to follow us…

The the **bitcoin address** used for the ransom payment is **created freshly** for every victim, so there’s no way to track it.

Just in case you are worried…

"Your privacy is important for us, all of your records including IP address and Encryption keys will be wiped out after your payment."


We Value Your Opinion
Watch later
How was Your Hacking Experience With Us?
★★★★★
★★★★
★★★
★★
★
Excellent
Good
Average
Poor
VeryPoor

UTPRESSINGSVARE

Vestas utsatt for datainnbrudd med krav om løsepenger

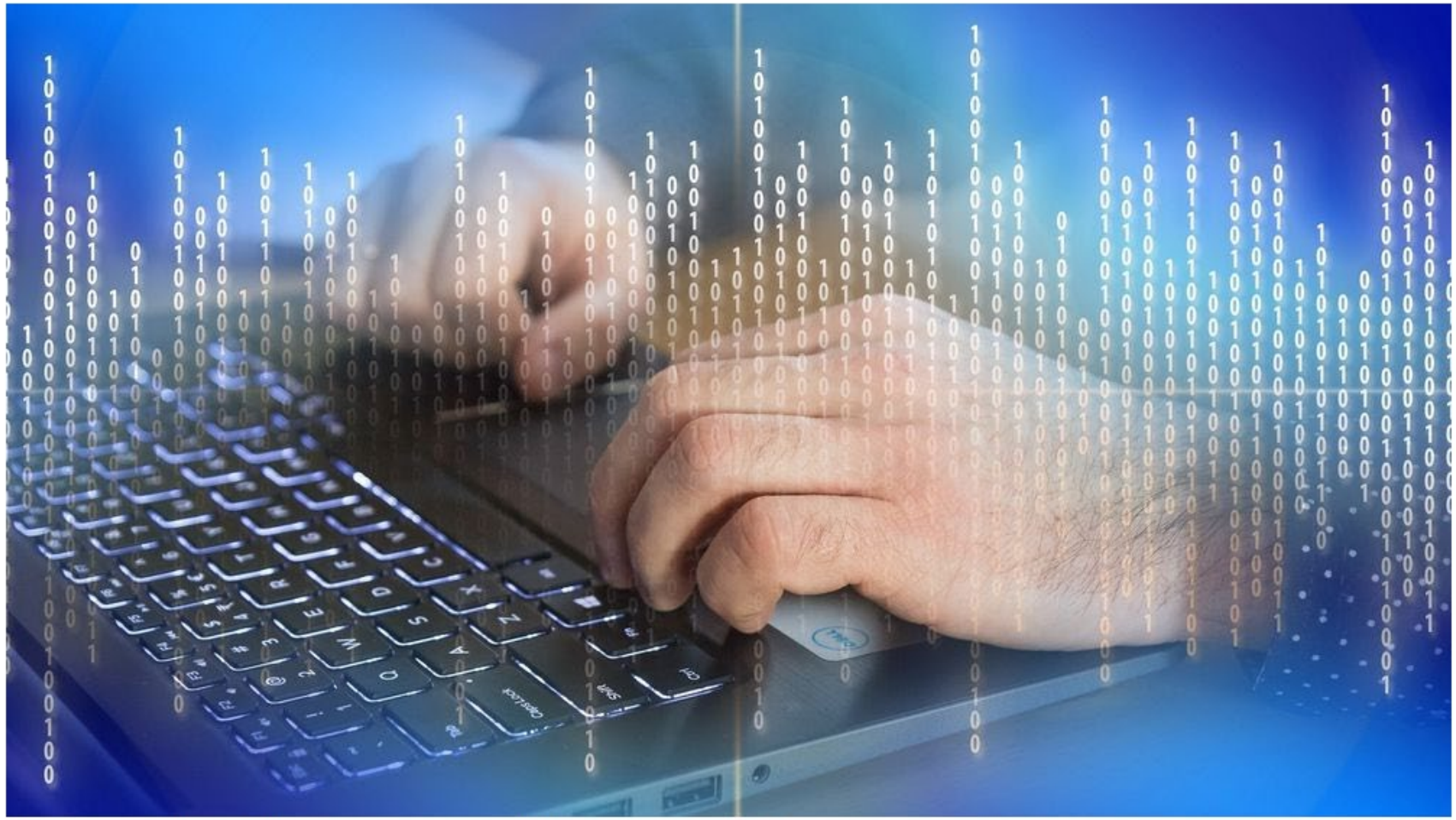
Hackere har slått til mot den danske vindmøllegiganten.

Det danske milliardkonsernet Vestas Wind Systems bekrefter at de er rammet av kryptovirus med krav om løsepenger. (Illustrasjonsfoto: Vestas)

MARIUS B. JØRGENRUD SIKKERHET 29. NOV. 2021 - 16:00

Denne skadevaren smetter unna nesten alle antivirusprogrammer

Sikkerhetsforskere hos HP advarer.



Ny skadevare distribuerer RAT-programmer og er vanskelig å oppdage, opplyser forskere. (Illustrasjonsfoto: geralt/Pixabay)

EIGIL KNUDSEN OPERATIVSYSTEMER OG PROGRAMVARE 28. NOV. 2021 - 19:00

The New York Times

Israel and Iran Broaden Cyberwar to Attack Civilian Targets

Iranians couldn't buy gas. Israelis found their intimate dating details posted online. The Iran-Israel shadow war is now hitting ordinary citizens.

Tel Aviv, Israel. The personal data of about 1.5 million Israelis were exposed in two recent hacks attributed to Iran. Jack Guez/Agence France-Presse — Getty Images

By Farnaz Fassihi and Ronen Bergman

Nov. 27, 2021

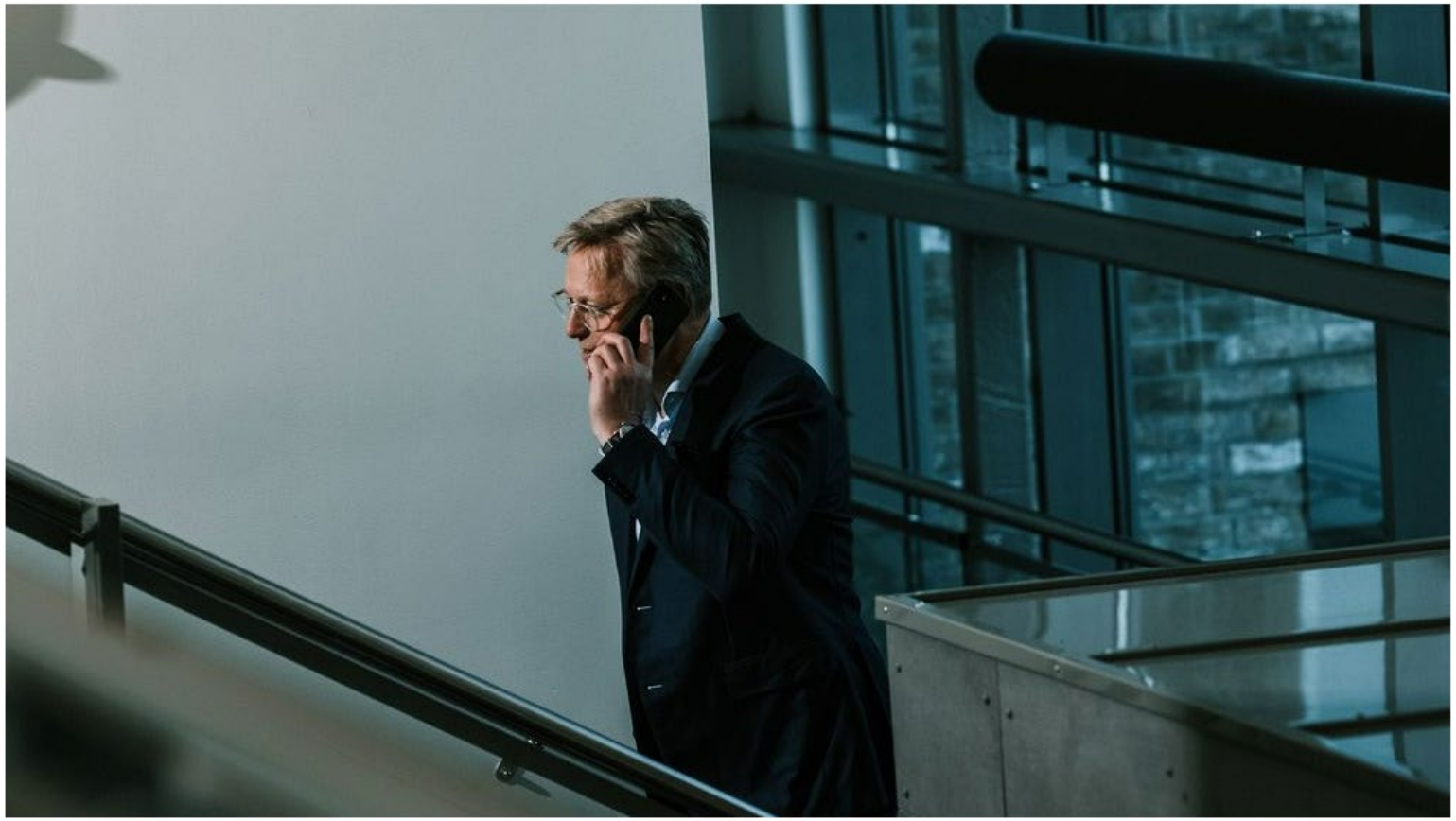
Nordic Choice Hotels rammet av datavirus

Nasjonal sikkerhetsmyndighet er varslet om det som har skjedd.

Nordic Choice Hotels er eid av Petter Stordalen.
Adam Ihse/ TT NYHETSBYRÅN

Nkom advarer mot massivt SMS-svindelangrep

Nkom ber ingen trykke på lenker de får i tekstmeldinger før de er helt sikre og advarer mot et storstilt svindelangrep som er i gang.



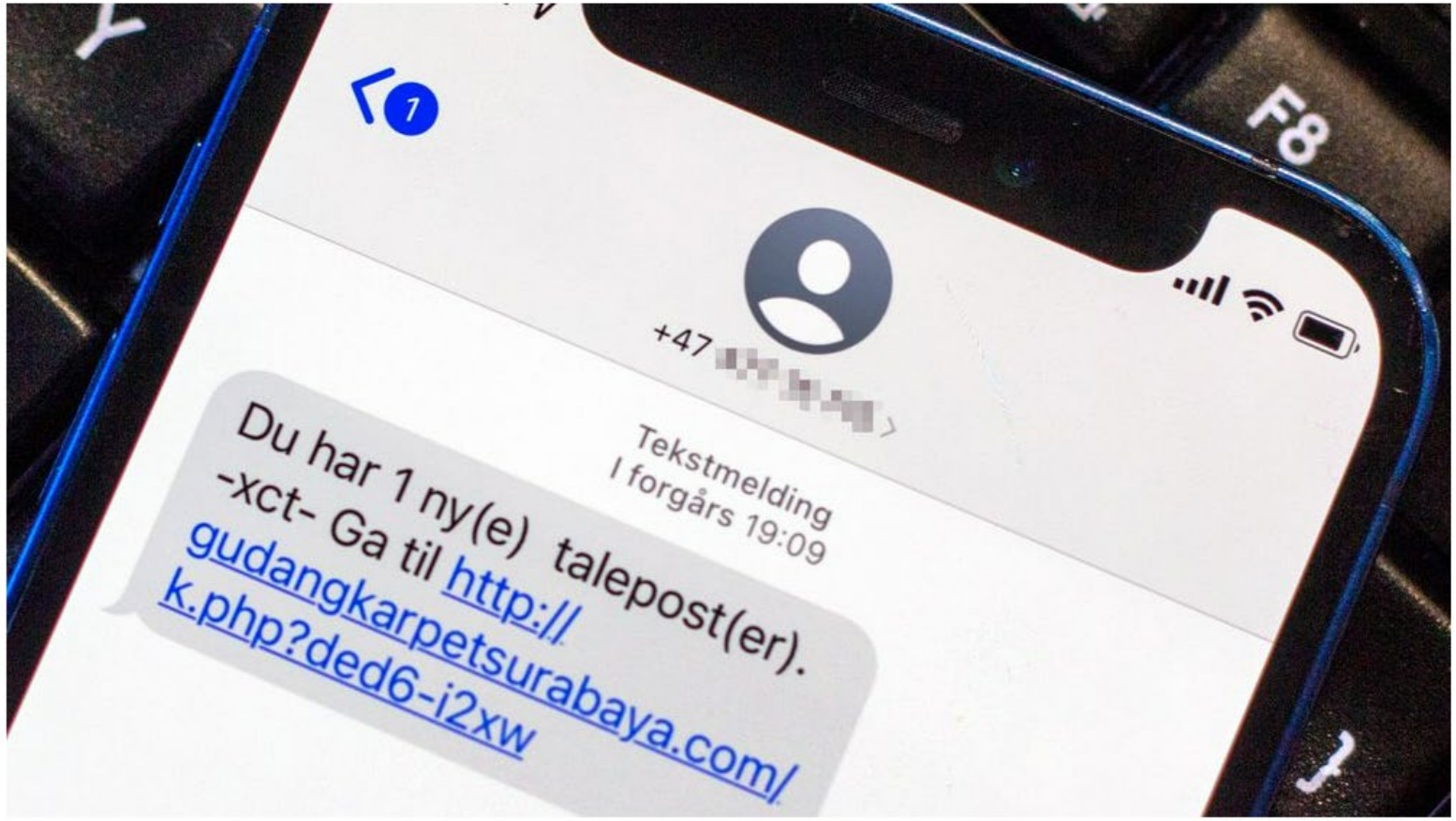
Pål Wien Espen i Nkom advarer mot massivt svindelangrep som nå rammer norske mobilbrukere. (Foto: Nkom)

NTB SIKKERHET 7. DES. 2021 - 16:39

ARTIKKELEN

Telia: Infiserte Android-telefoner sprer tusener av SMS i minuttet. Slik lurer de også Iphone-brukere

Svindelbølgen viser ingen tegn til å avta.

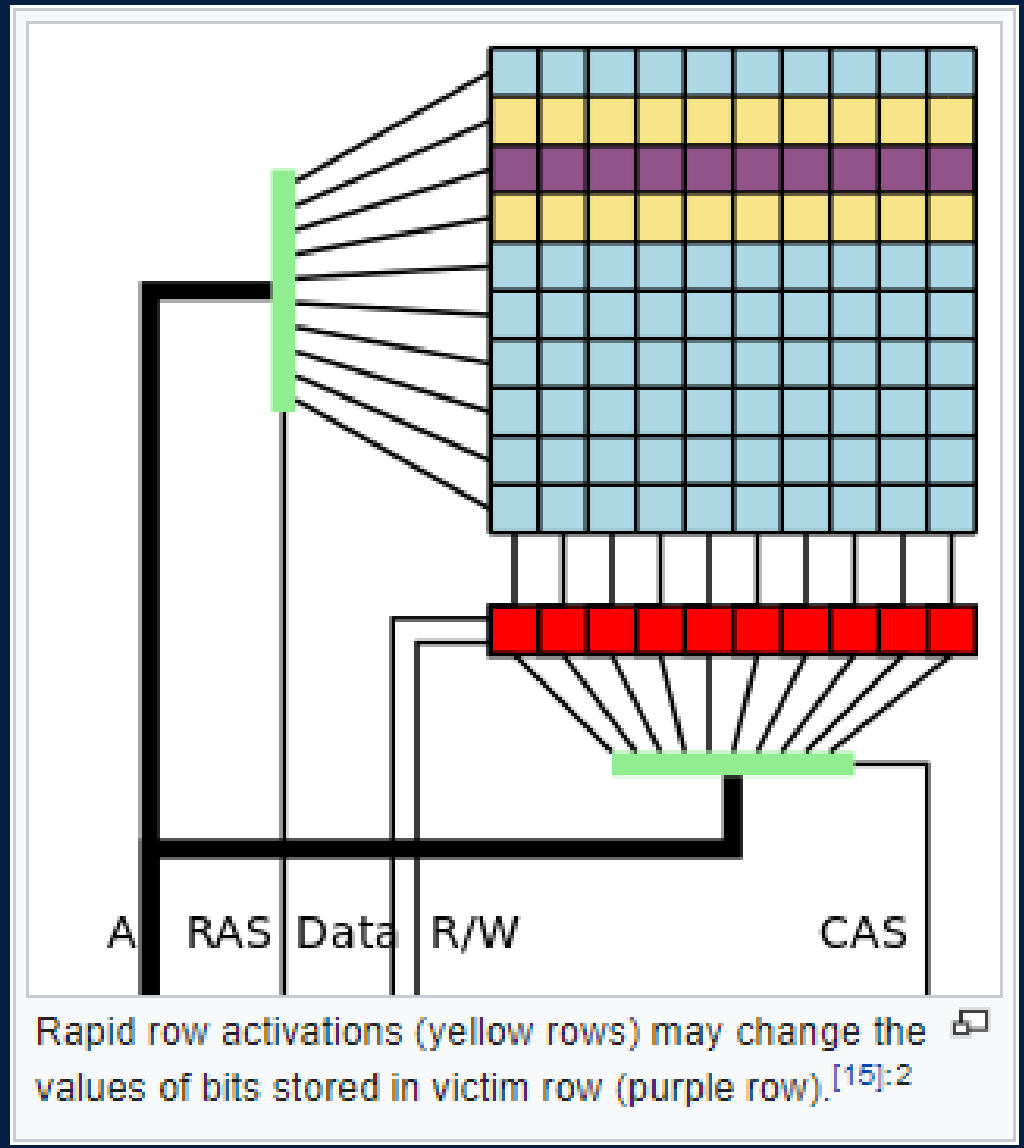


Flubot prøver typisk å lure mottakerne med påstand om talepost eller sporing av pakker. Kampanjen spres nå fra norske telefonnumre. (Foto: Are Thunes Samsonsen)

Rowhammer (2014)

- Physical issue where rapid rewrites of data in DRAM can change the state of a near row.

- Blacksmith 2021 (exploit) proves no memory is safe. As a result all modern computers technically can be hacked if the attacker is left to do the attack undisturbed.



Rapid row activations (yellow rows) may change the values of bits stored in victim row (purple row).[15]:2

Defense Measures

- In order to defend against an attack or being lured into a phishing attack it is important to be vigilant.
- We have implemented defense measures, we will continue to improve these and require your assistance and understanding.

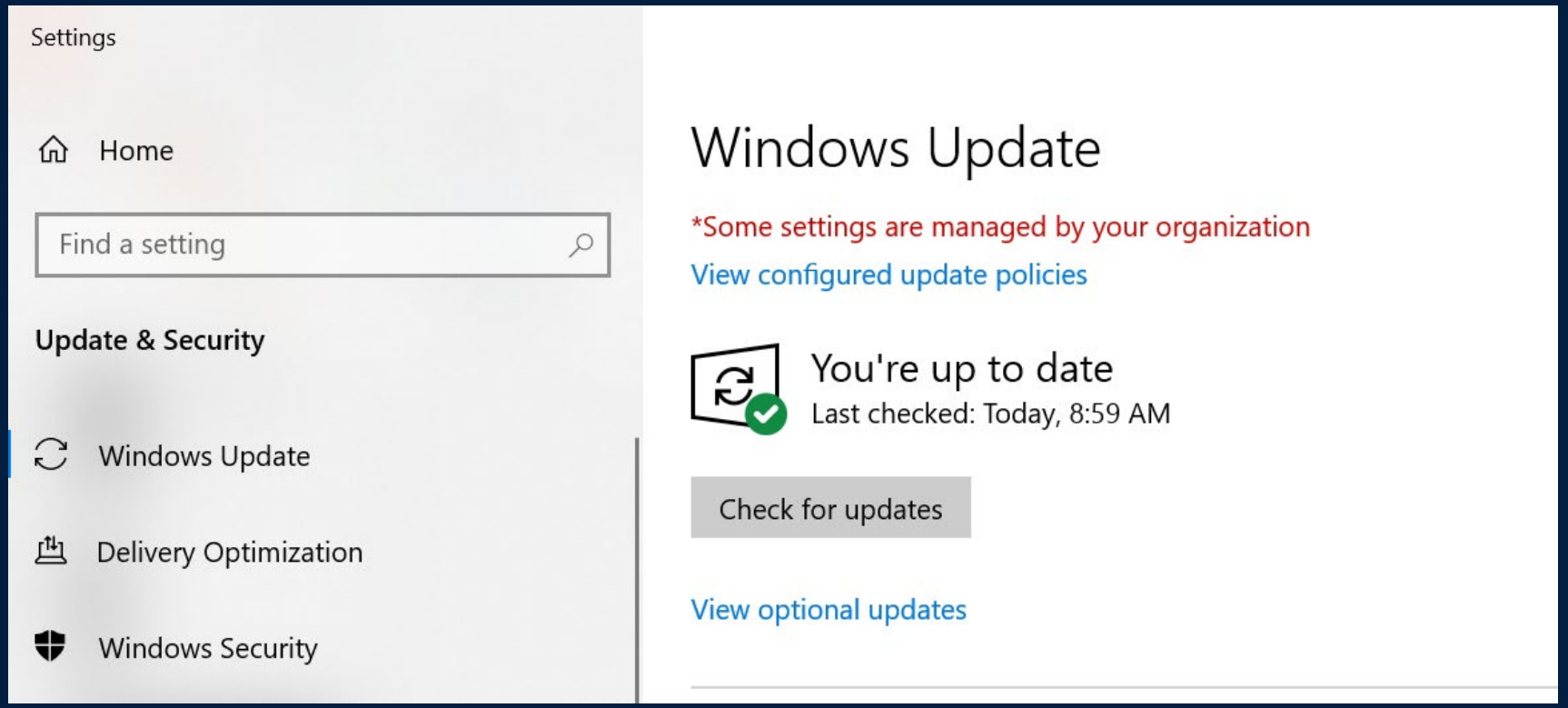
- Nanolearning; follow the link on the intranet:
- IT-sikkerhet – ScaleAQ Intranet

Nano leksjoner

- ✓ Digital Sikkerhet
- ✓ Vær en STAR i covid-19-tiden
- ✓ Sjekk alle lenker
- ✓ Beskytt nettverket på hjemmekontoret
- ✓ Hold deg på den sikre siden på telefonen
- ✓ Hvordan ligger vi an med STAR-atferd? (nr. 1)
- ✓ Vær en STAR: Stopp opp og tenk
- ✓ Sjekk alltid avsender og innhold
- ✓ Beskytt kontoene dine
- ✓ Hold deg på den sikre siden i skyen
- ✓ Vær en STAR: Spør og reager
- ✓ Sjekk alle fakta
- ✓ Beskytt deg og oss mot løsepengevirus
- ✓ Hold deg på den sikre siden i det offentlige rom
- ✓ Hvordan ligger vi an med STAR-atferd? (nr. 3)
- ✓ Digital sikkerhet: Risikovurdering

STAR – Stop – Think – Ask - React

Update of Operating system

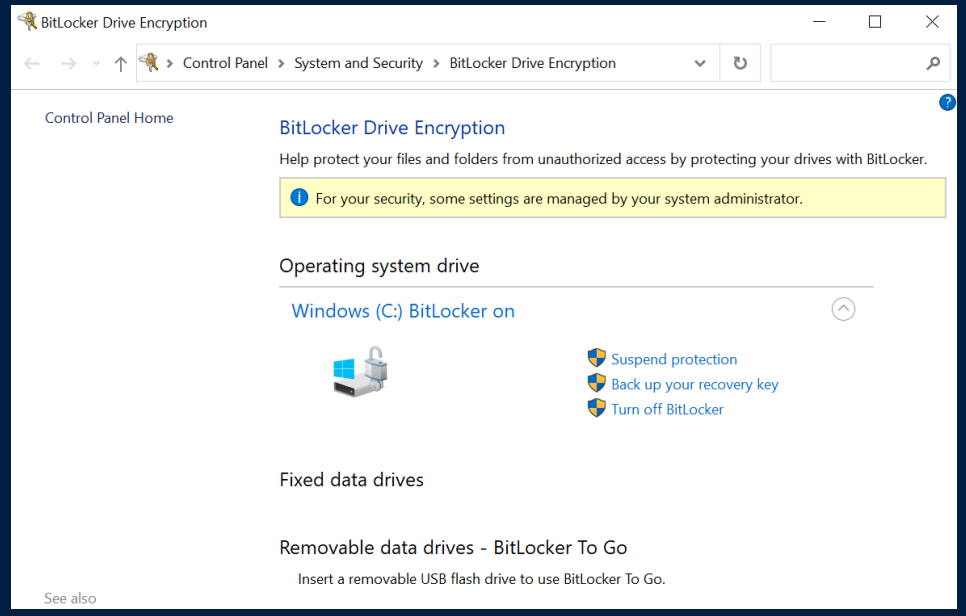


Update of Mobile Operating System

Turn on Automatic Updates on company devices

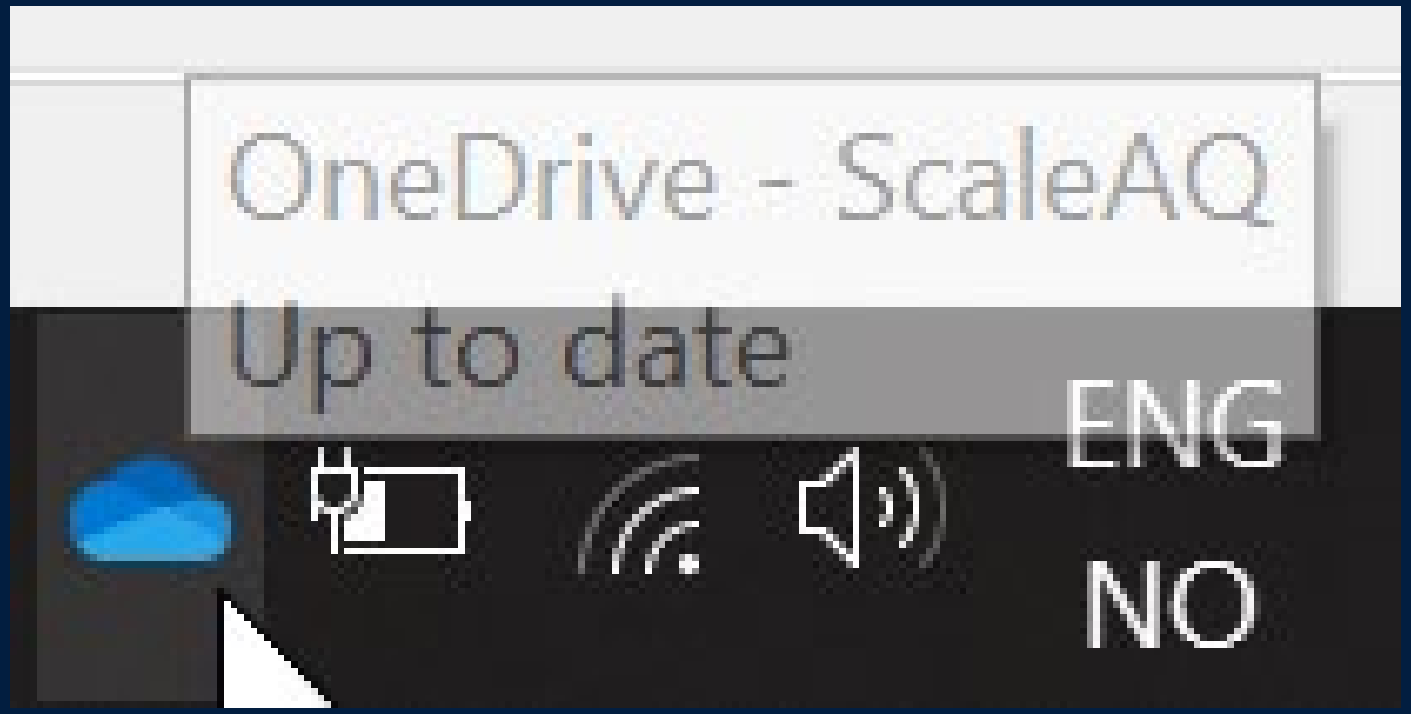
Bitlocker

- All computers required to have the storage devices encrypted.
- This makes attacks harder and prevents access if device is stolen or lost.
- 140 computers unencrypted. Will be contacted with instructions shortly after this meeting.

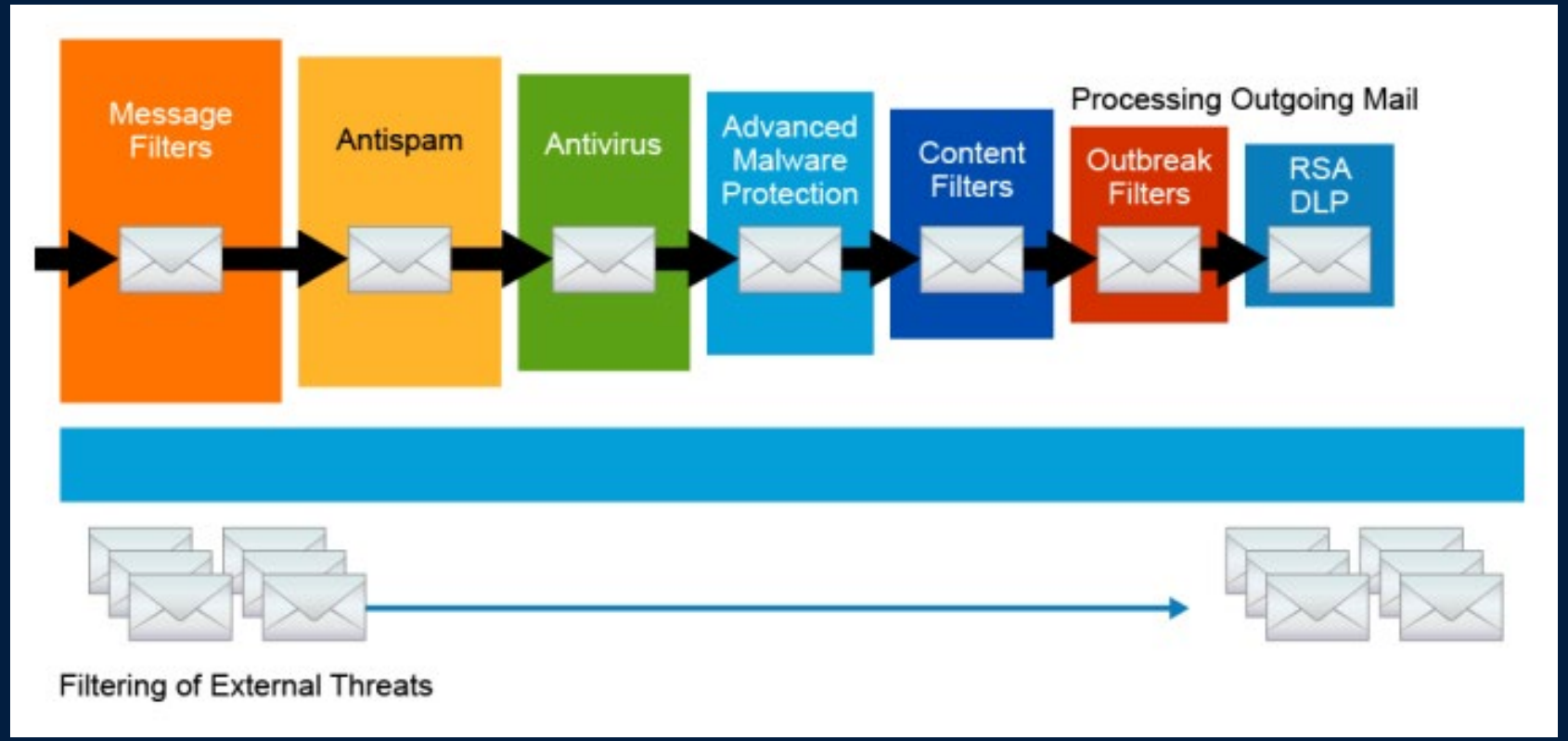


Use Sharepoint and OneDrive for your documents

- Data is much safer in the Cloud. Make sure you do not save and work only on documents locally on your PC. They will be lost if device is lost, hacked, crashes.



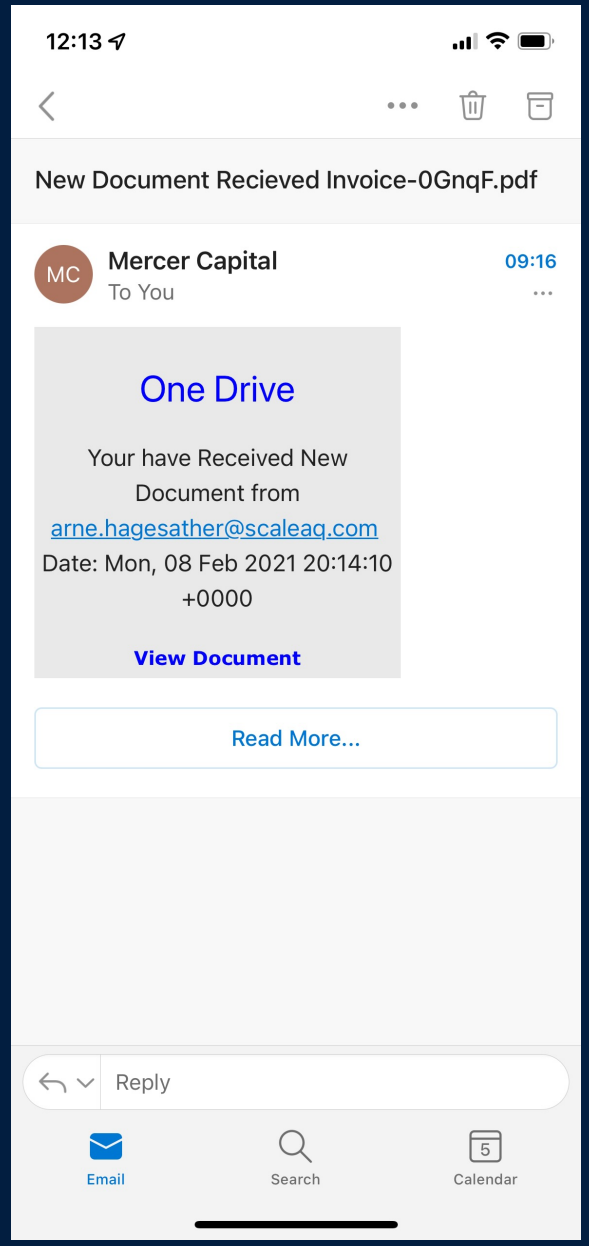
Email Scanning



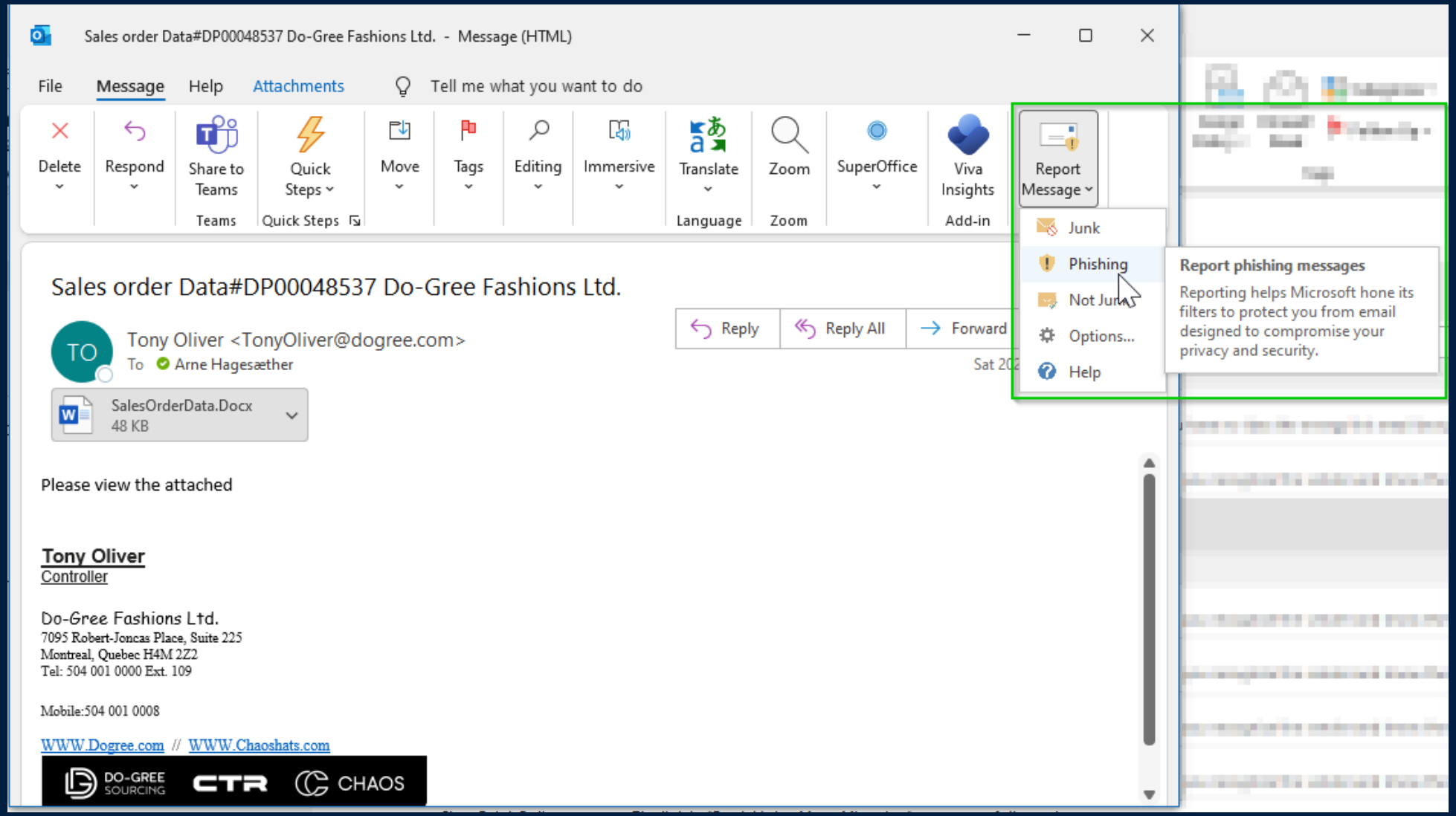
Still some emails delivered might be phishing

- To combat this user training is needed.
- We will be launching phishing campaigns
- One was run before this SpeakUP

Phishing Test

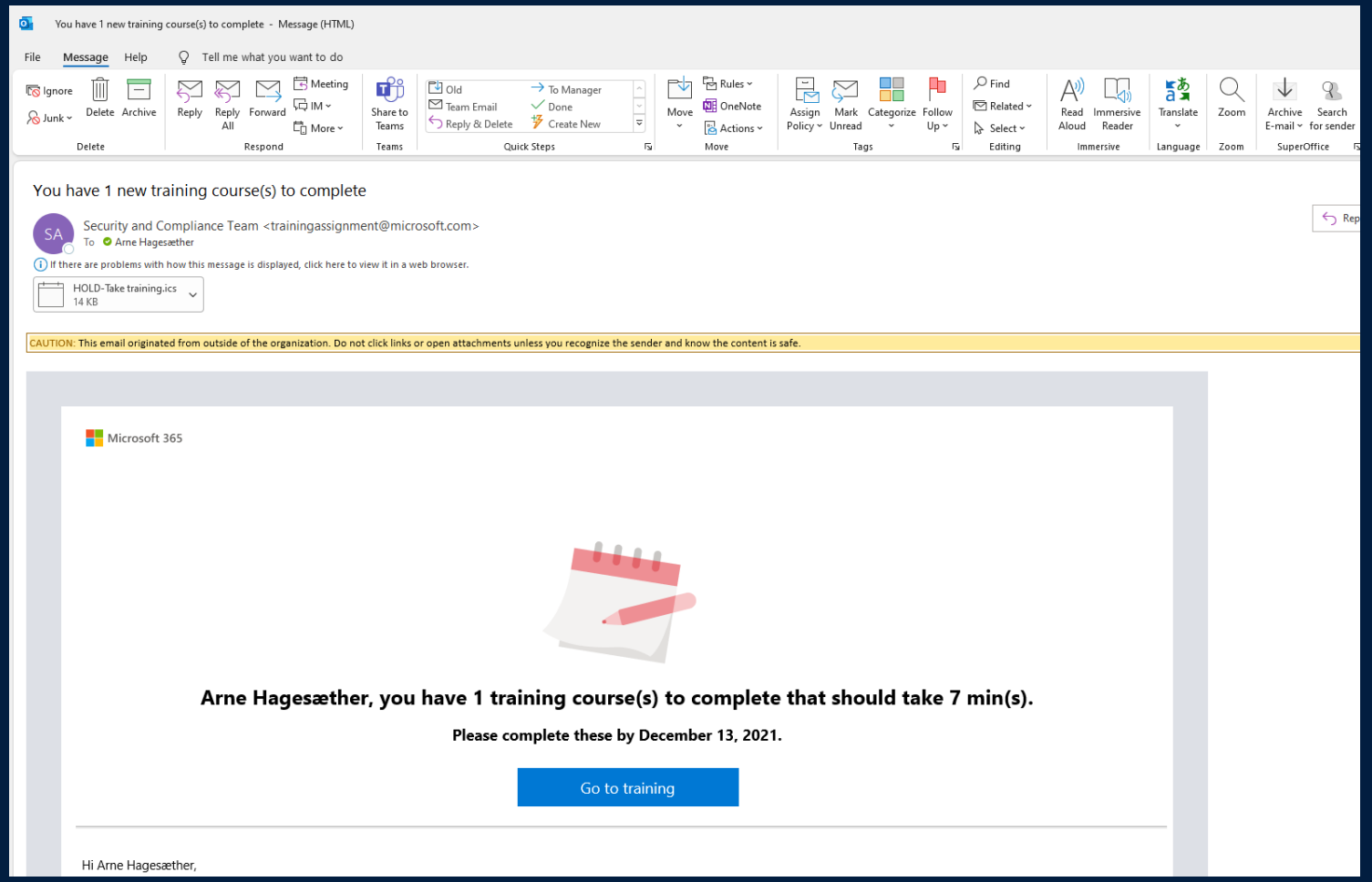


Report Phishing



Phishing Training

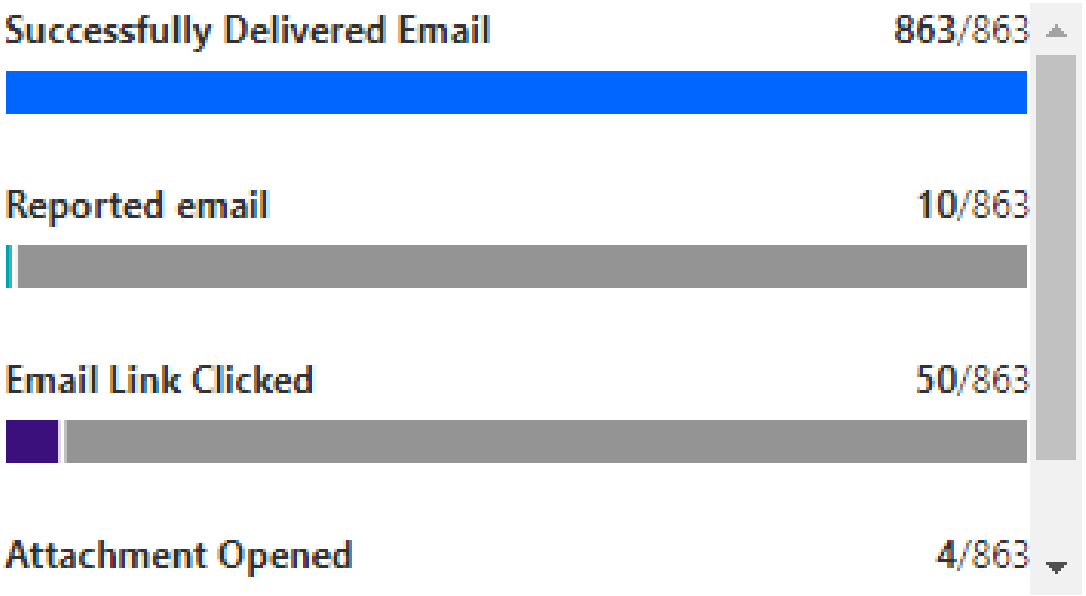
- If you got phished you will get training from Microsoft.com



Phishing results

All user activity

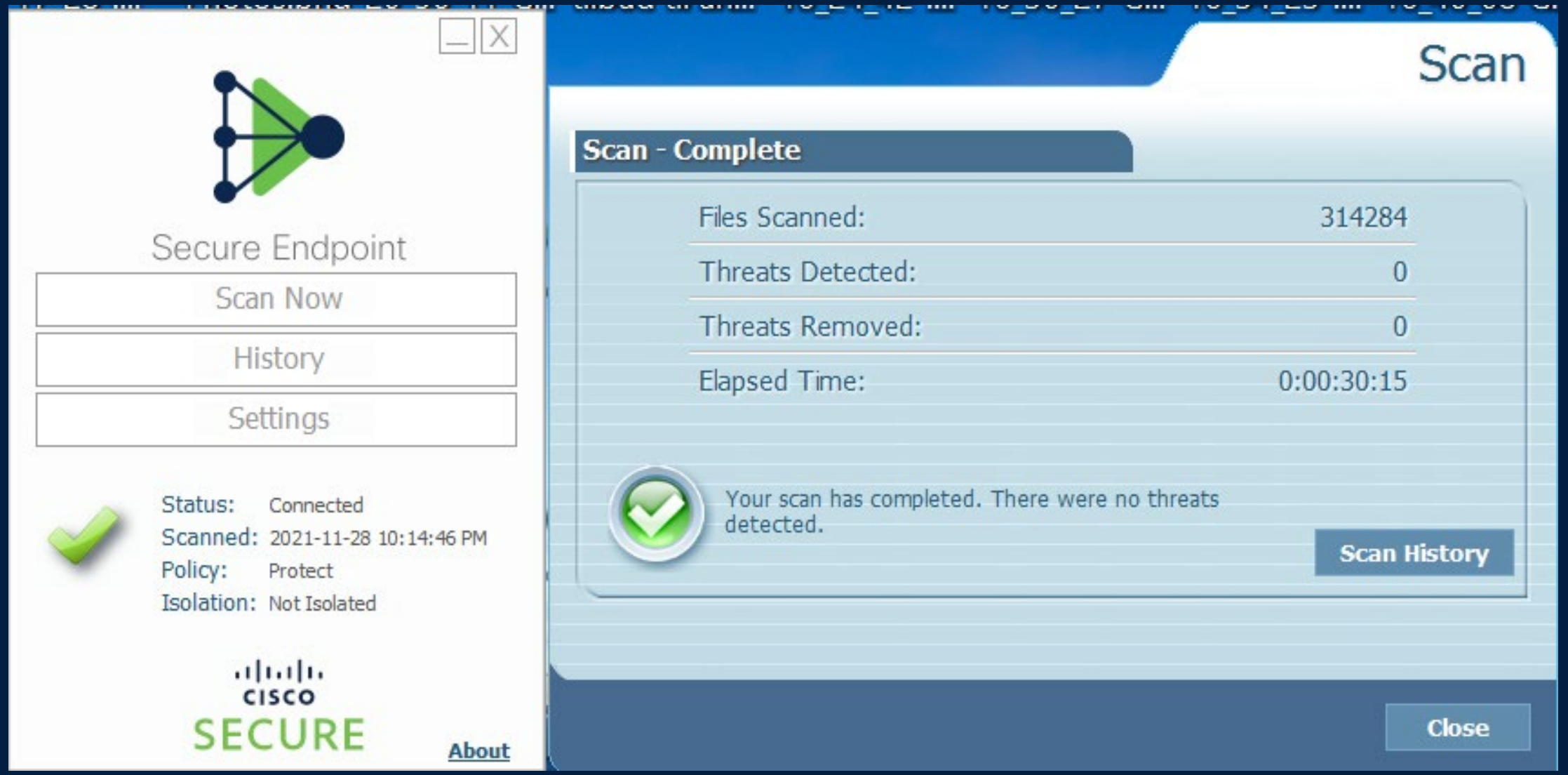
4 of 863



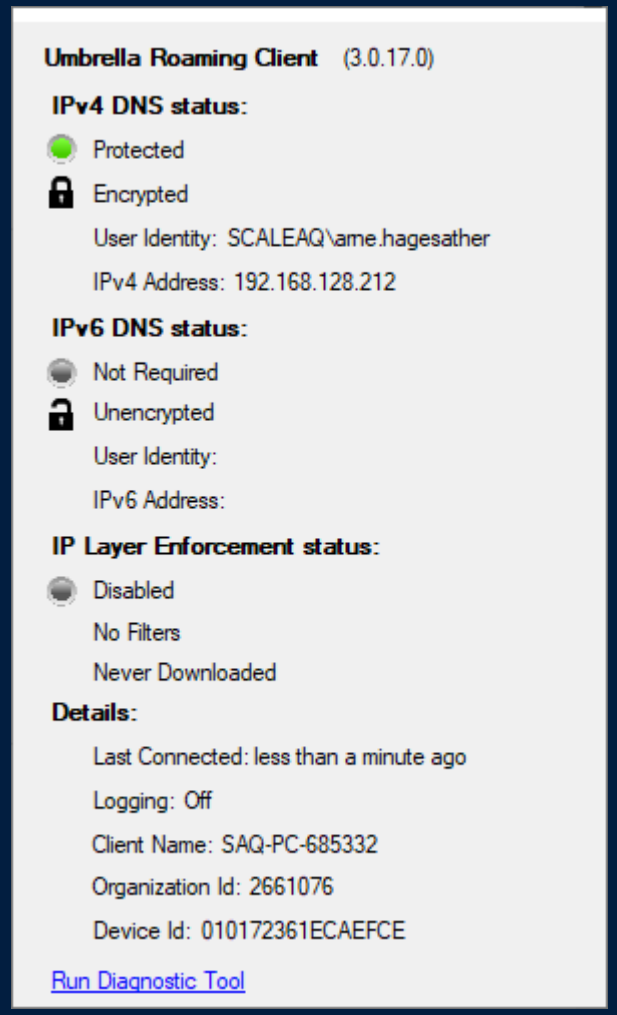
Training completion

9 of 50 users completed training

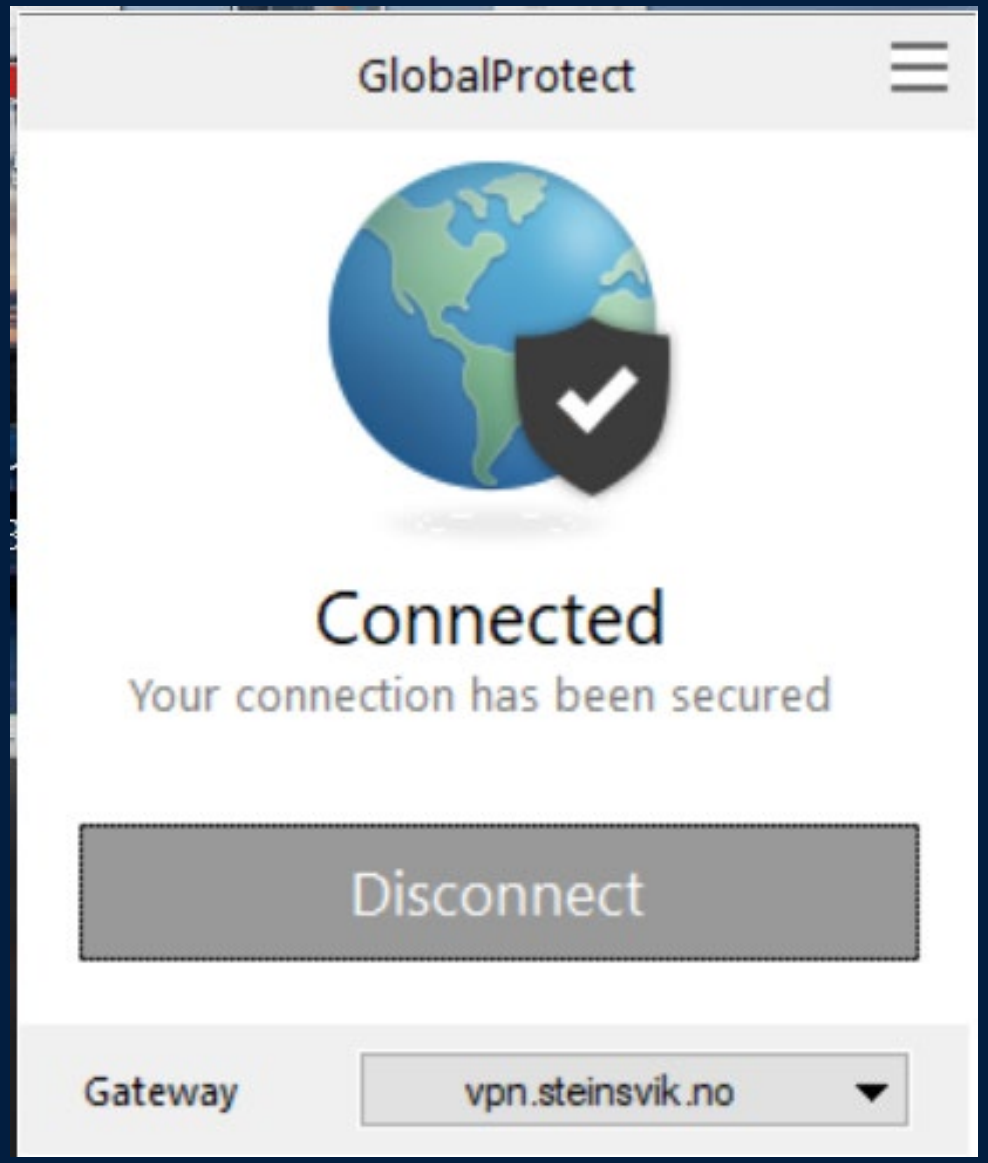
Cisco Secure Endpoint protection



Umbrella Roaming Client



Use VPN when outside the Office



Umbrella Roaming Client works together with VPN

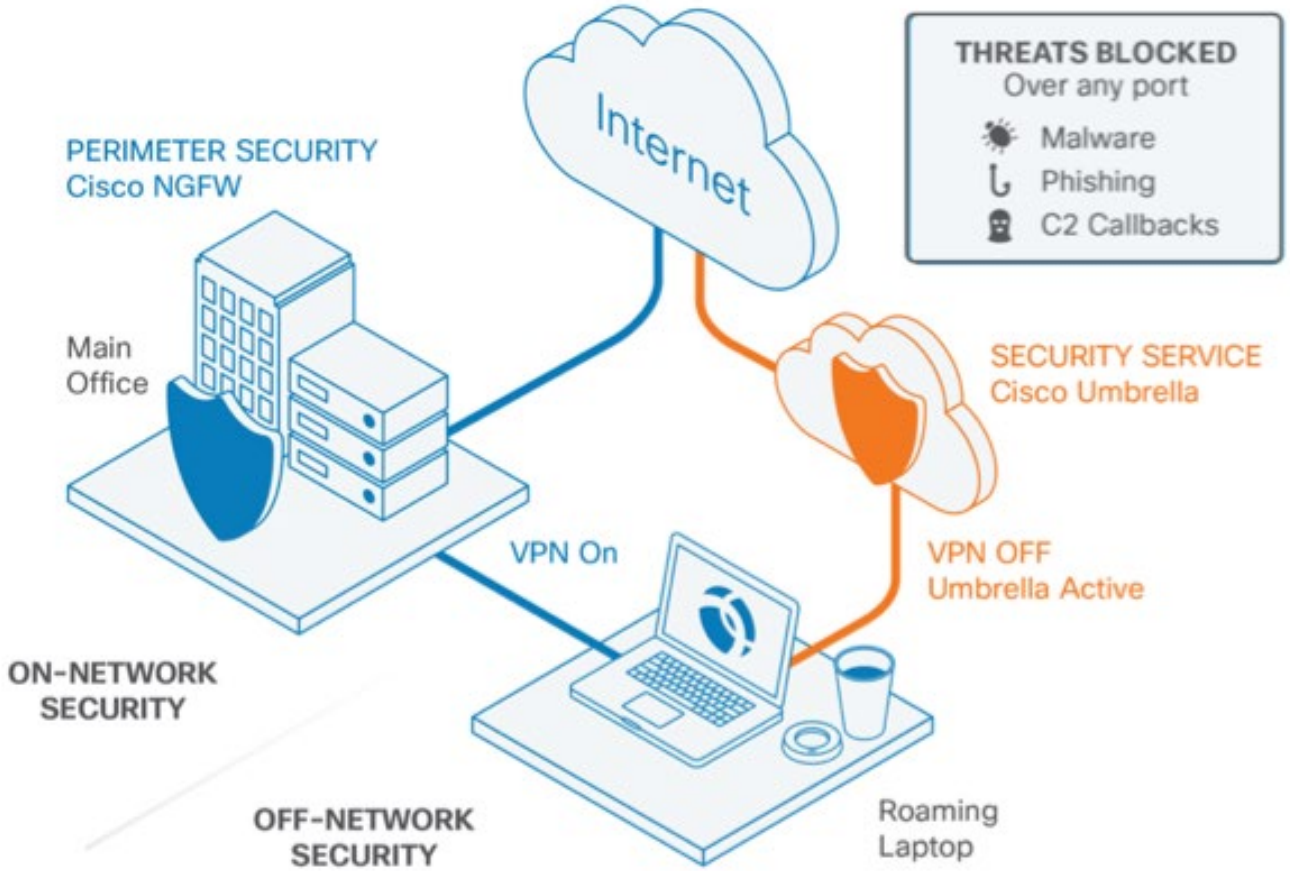


Figure 1: RC through the VPN — Source

Password

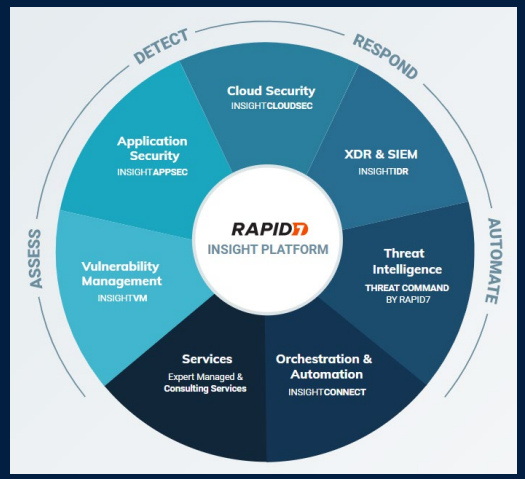
- Make the password strong
  - It is a computer trying to guess them. Use a sentence
- Do not use the same password on other sites.
  - If one gets hacked they have them all.
- How difficult is a password to crack?
  - https://www.passwordmonster.com/

MFA – Multi Factor Authentication

- MFA should be enabled on all external services.
  - MFA protects against stolen credentials
  - It requires not only credentials but phone to be stolen as well
  - Microsoft Authenticator is safer than SMS messages
- Hide notifications on your phone when it is locked. If your phone is stolen make sure the two factor code is not displayed with the phone is locked.

Security Operation Centre (TBA)

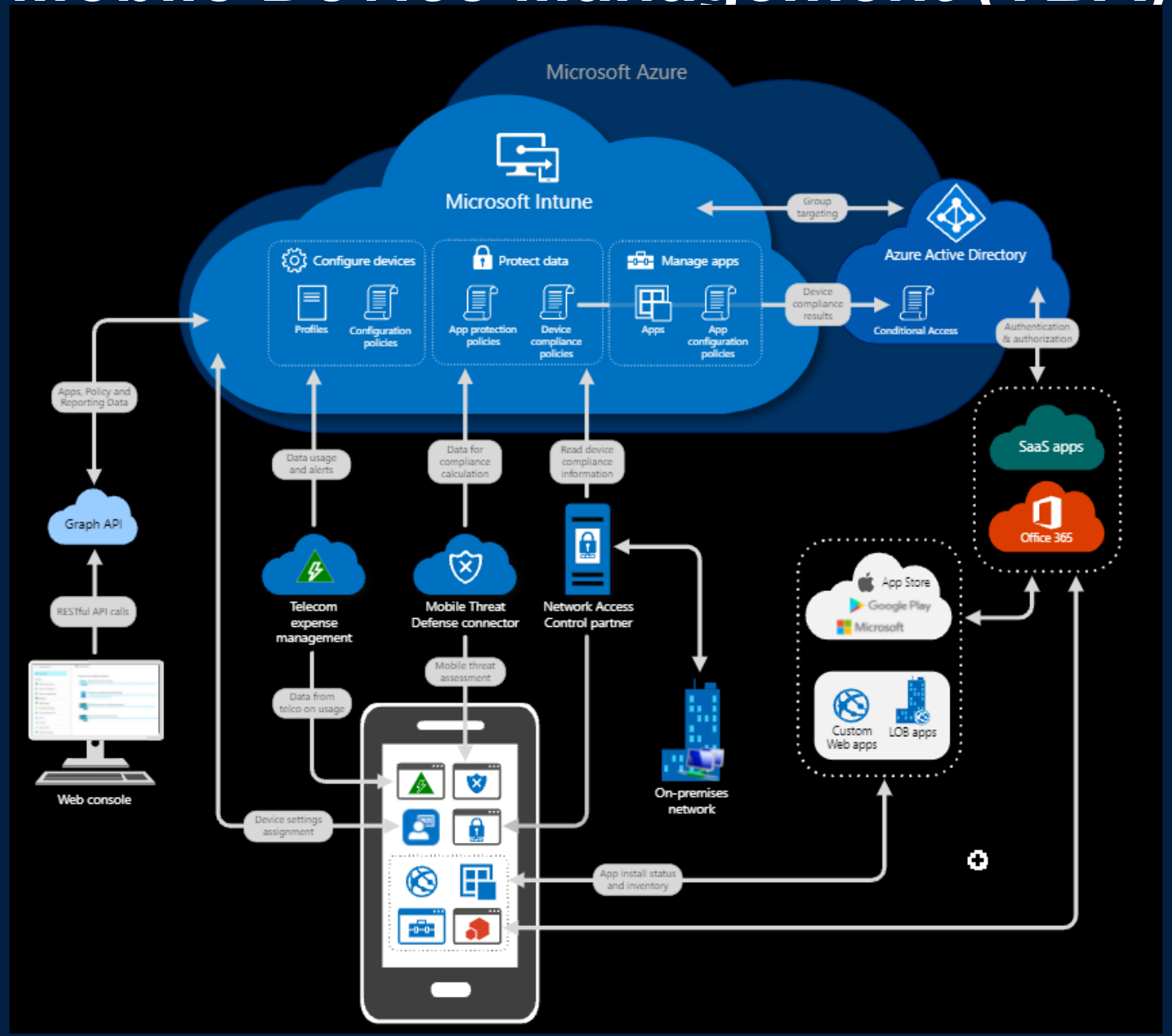
- We have signed up for a service for a Security Operation Centre by Visolit. Rapid7 is used by 9900 customers, including 45% of the Fortune 100 (USA).
- They will monitor and prevent attacks
- Startup project meeting this week
- One escalation phone number
- More information will be posted on the intranet



Mobile Device Management (TBA)

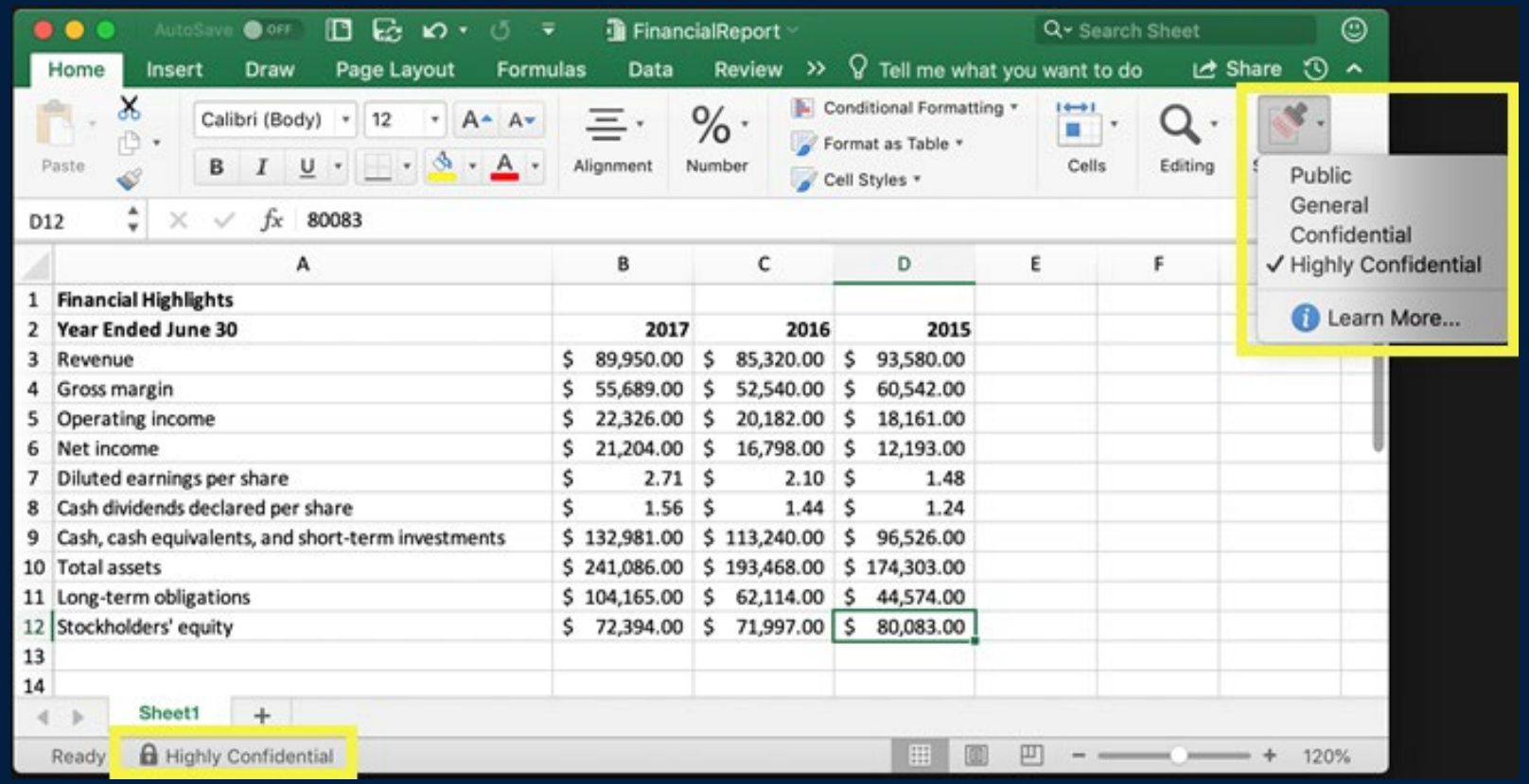
- Company mobile phones to be enrolled in intune
- Lock lost devices
- Remote wipe stolen devices
- Split company applications with private application
- Wifi works in all office locations (Ability to push wifi keys)
- Data Loss Prevention (DLP)
- Publish applications (Such as ERP, Dynamics 365)
- OS version update
- Prevent jailbreaked devices
- Note: Location data collected, installed applications might be collected. However there is audit log and IT will not use.

Mobile Device Management (TBA)

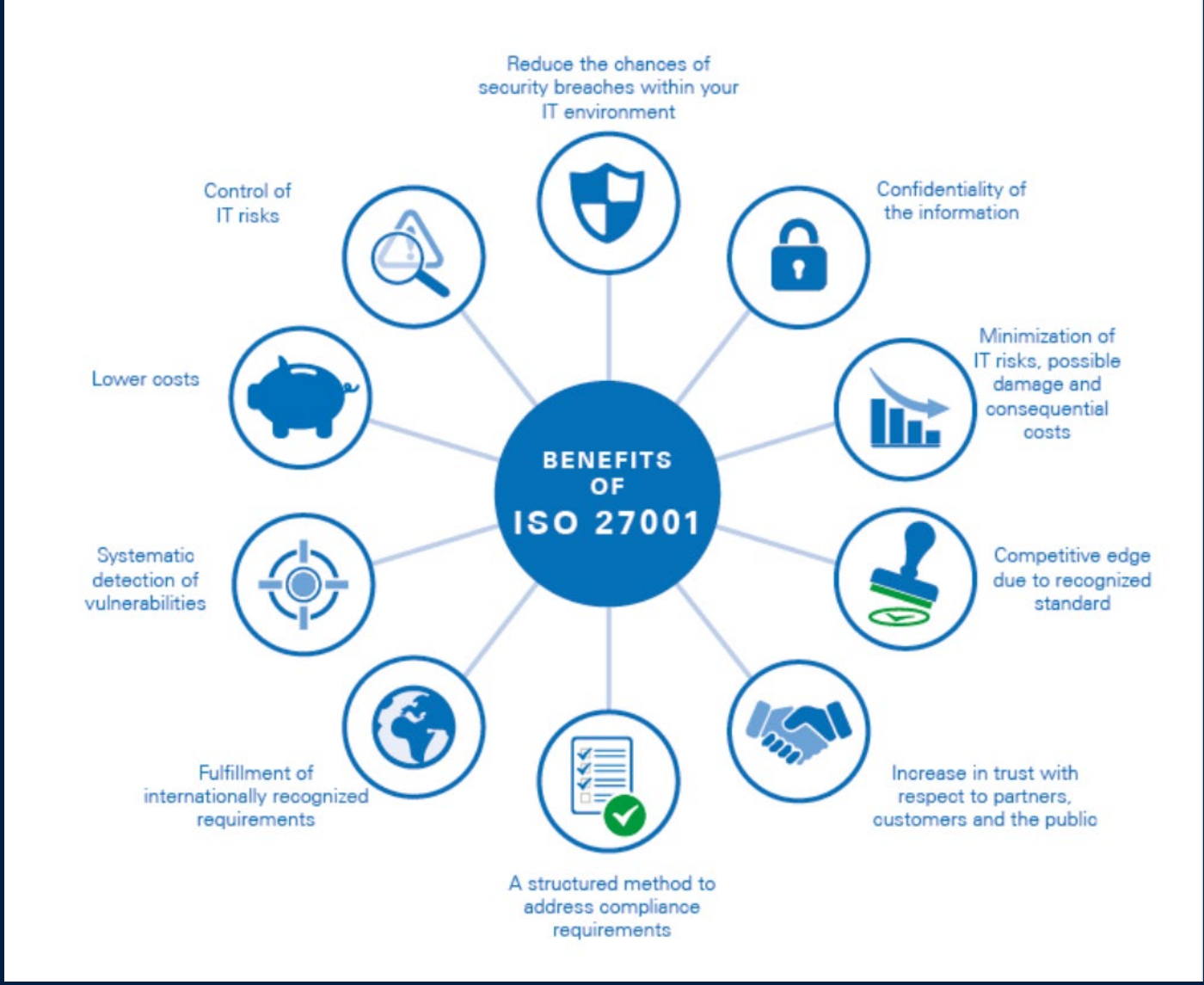


DLP – Data Loss Prevention (TBA)

- Sensitivity labels
- Prevent mishaps where internal documents are sent to external parties



ISO 27001 (TBA)



Protect your home network

Beskytt nettverket på hjemmekontoret

Ifølge undersøkelser vil covid-19 kunne føre til en dobling av permanente hjemmearbeidende.

Du har et ansvar for nettverkssikkerheten på ditt hjemmekontor.

Det høres kanskje skummelt ut, men **enkle tiltak** kan utrette mye. Har du for eksempel noen gang tenkt på å slå av wi-fi før du legger deg?

Les om hvordan vi kan **beskytte hjemmenettverk**.

Protect your home network

Det trådløse hjemmenettverket

Hjemmenettverket er konfigurert med en **ruter** som gjør at du kan koble flere enheter til internett.

Men selv om ruteren er viktig for sikkerheten, kan dens egenskaper og standardinnstillinger faktisk gjøre det enkelt for inntrengere å få tilgang til nettverket og **tilkoblede enheter**.

Og når de først er kommet inn, kan de overvåke aktiviteten, stjele data eller misbruke kontoene dine. De kan kjøre skadelig programvare – eller kanskje legger du aldri merke til dem overhodet.

Protect your home network

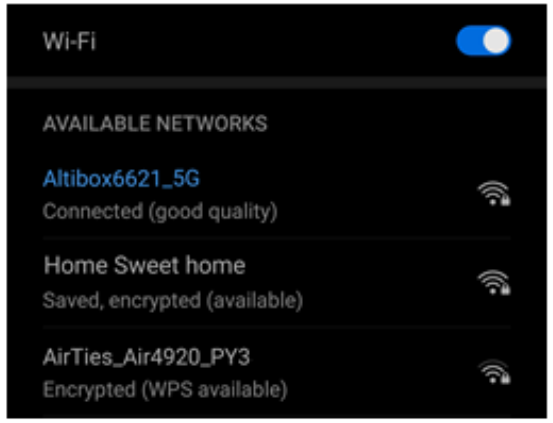
Grunnleggende nettverksbeskyttelse

Du må først gå inn på ruterens/nettverkets **innstillinger**. Se ruterdokumentasjonen eller brukerprofilen din hos internettleverandøren.

1. Erstatt alle standard **passord** for hjemmenettverket og for administrator-pålogging med sterke, unike passord.

2. Endre **nettverksnavnet**. Standard ruternavn kan avsløre produsenten eller internett-leverandøren og slik røpe kjente sårbarheter. Angi et navn du kjenner igjen, men som ikke avslører personopplysninger.

3. Aktiver **nettverkskryptering** (WPA2 eller 3) og automatiske **programvareoppdateringer**.



Protect your home network

Grunnleggende enhetsbeskyttelse

Tom har to PC-er, et nettbrett, en telefon og mengder av annet utstyr som kobles til internett via familiens nettverk. Og to grinete tenåringer som holder på med sitt.

Så langt har han iverksatt to gode tiltak:

1. Installert **antivirus** og brannmurer på begge Windows-PC-ene.

2. Sagt til sønnene at de skal bruke sterke **passord** og aldri det samme på to steder.

Det er mye vi kan gjøre for å sikre enheter bedre, men vi forventer at du som et minimum har stell på antivirus og passord i hjemmet.

Recommendation to update Firmware on your personal wifi router

Thousands of Netgear routers can be hacked — here's what to do

By Paul Wagenseil September 21, 2021

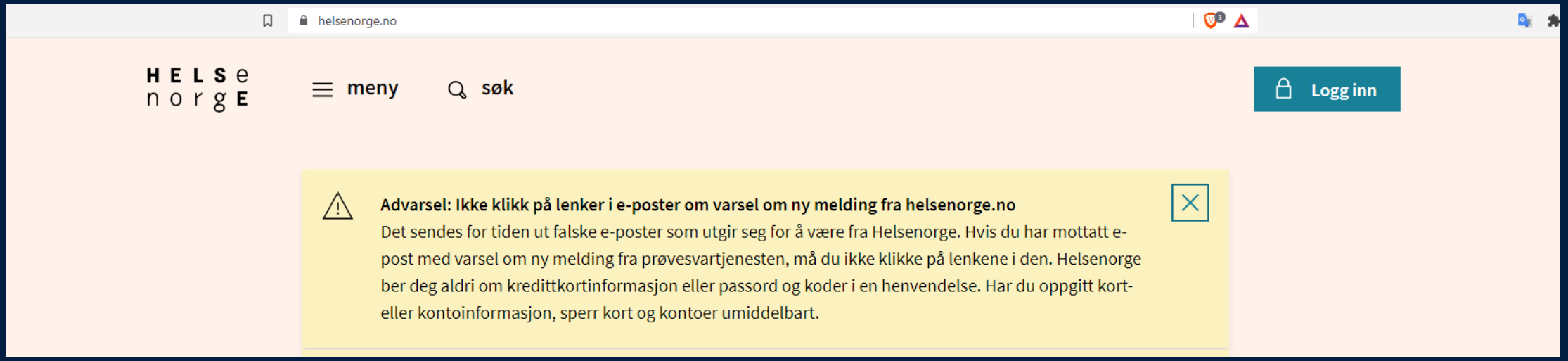
At least 11 different Netgear Nighthawk models are vulnerable

Comments (0)

(Image credit: Netgear; Shutterstock)

[Security Advisory for Remote Code Execution on Some Routers, PSV-2021-0204 | Answer | NETGEAR Support]

Do not click on any links. Go directly to their site



Trygg og smart julehandel

Julen nærmer seg, og det er høysesong for handel både på nett og i butikk. Derfor har vi samlet noen enkle tips og triks for en trygg og smart julehandel.

Kortinformasjonen din er nå tilgjengelig i appen og nettbanken – det betyr at du kan handle på nett uten å måtte finne frem lommeboken. Her kan du lese mer om ditt digitale kort.

Fem råd når du handler på nettet:

1. Handle hos kjente aktører eller i lokale nettbutikker, så er sjansen for å bli lurt mindre. En annen fordel med lokale nettbutikker er at du også støtter det lokale næringslivet.
2. Hør med familie eller venner, eller gjør et raskt google-søk for å se om andre har gode erfaring med butikken. Dersom noe virker for godt til å være sant, så er det ofte det.
3. Betal med Visa Gull – da er du dekket dersom du ikke skulle motta varen eller om leverandøren går konkurs.
4. Sjekk at du finner kontaktinformasjon og opplysninger om kundeservice på nettsiden. Hvis ikke bør du styre unna
5. Skal du handle på nett så se etter hengelåsikon eller bokstavene HTTPS til venstre i adressefeltet, da vet du at tilkoblingen er sikker.

Use common sense when using your work computer

- Do not install software from unknown sites
  - Use Company Portal to install software. Contact itsupport@scaleaq.com for help.
- Don’t use memory sticks for example to share documents from private computer to work computer
- Do not install Games on your work laptop
- Do not buy or sell Crypto currencies from your work laptop
- Do not visit porn sites
- Do not visit gambling sites
- Do not visit alcohol sites
- All above can be an HR case for breach of IT Policy

Stay Safe!

Use your work computer for work purposes ☺