

A glowing green padlock is centered on a dark blue background with a complex, glowing circuit board pattern. The padlock is illuminated with a bright green light, making it stand out against the darker, blue-toned background. The circuit lines are thin and intricate, creating a sense of digital connectivity and security.

IT Security

Arne Hagesæther



The Attack

Remote
Platform
Hacking



Email
Phishing
Schemes

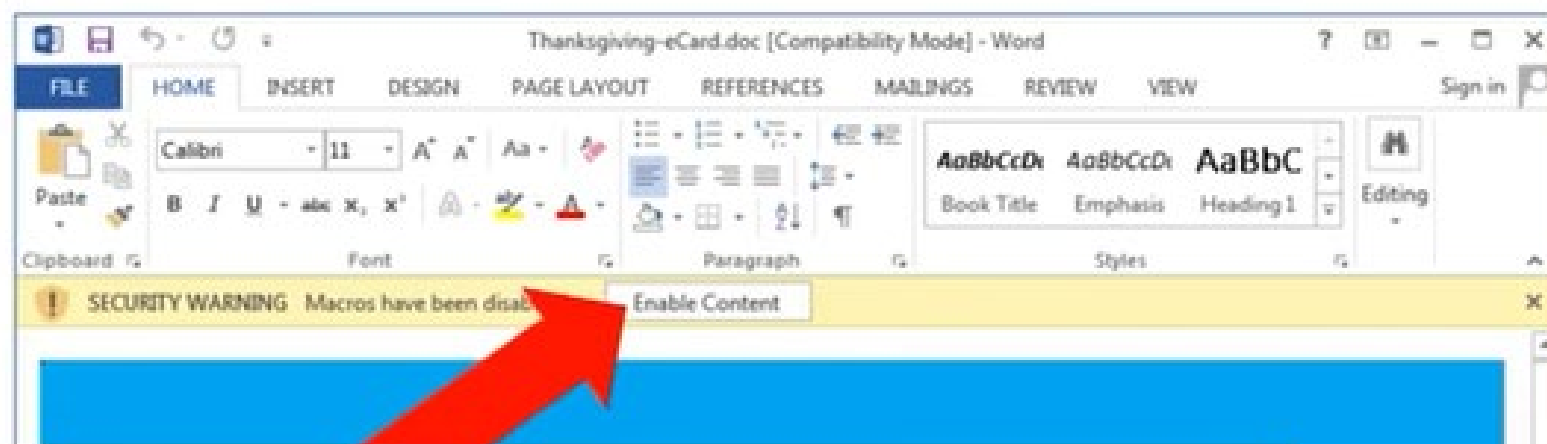


Compromised
Employee
Credentials





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.



payment document 464719.d...

157 KB



resume



Jeff Lanza

Today, 7:52 AM

Jeff Lanza ▾



Reply all ▾

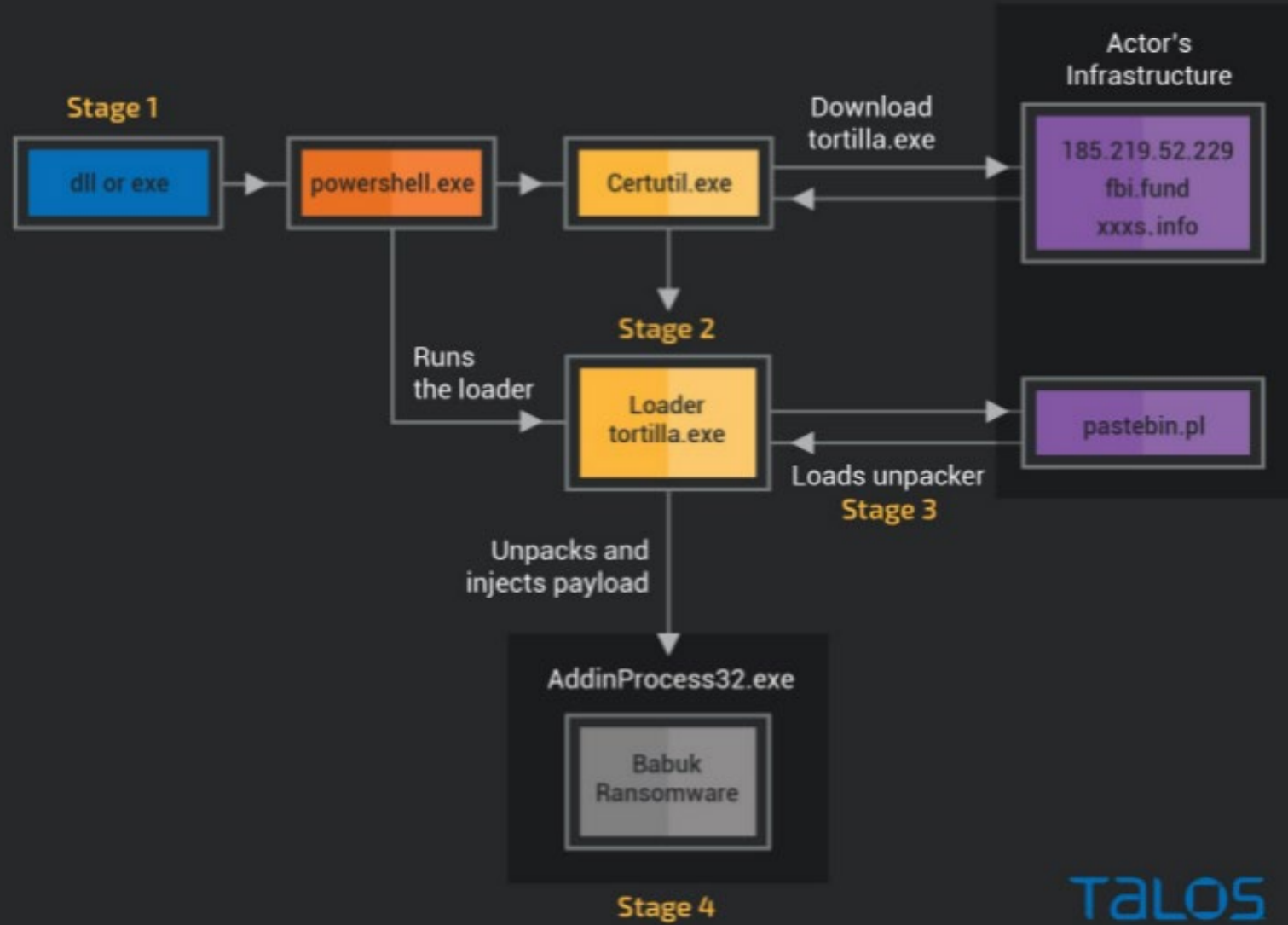
<https://www.dropbox.com/s/mtorrewyka41l7o/resume.pdf?dl=0>



resume.pdf

www.dropbox.com

Shared with Dropbox



Infection flow-chart.



2. The Encryption



_Decrypt_Files.html



_Decryption_ReadMe.html



_Help_Help_Help.html



_Help_Important.html



Encrypted_0b33984133925505.enc_robbinhood



Encrypted_0d5b2c8e9204b3ff.enc_robbinhood



Encrypted_0e60f2d5f437b31f.enc_robbinhood



Encrypted_01bd693ee8385913.enc_robbinhood



Encrypted_1ceb7507cf3c128d.enc_robbinhood



Encrypted_1e1e37262ce1b36e.enc_robbinhood



Encrypted_1eb34d9a763cd05b.enc_robbinhood



Encrypted_02af6183882ff462.enc_robbinhood



Encrypted_2b416abf3332ff56.enc_robbinhood



Encrypted_3a020812ec9c51e0.enc_robbinhood



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_\(cryptosystem\)](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.”



IDEAN

We Value Your Opinion

Watch later Sh

How was Your Hacking Experience With Us?



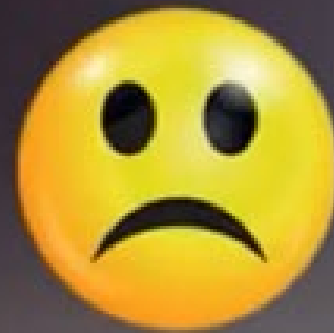
Excellent



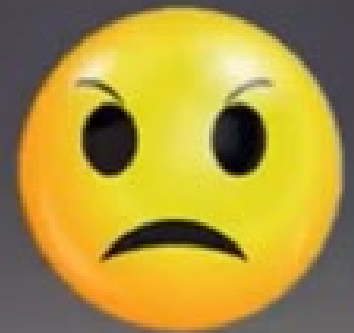
Good



Average



Poor



VeryPoor

Vestas utsatt for datainnbrudd med krav om løsepenger

Hackere har slått til mot den danske vindmøllegiganten.



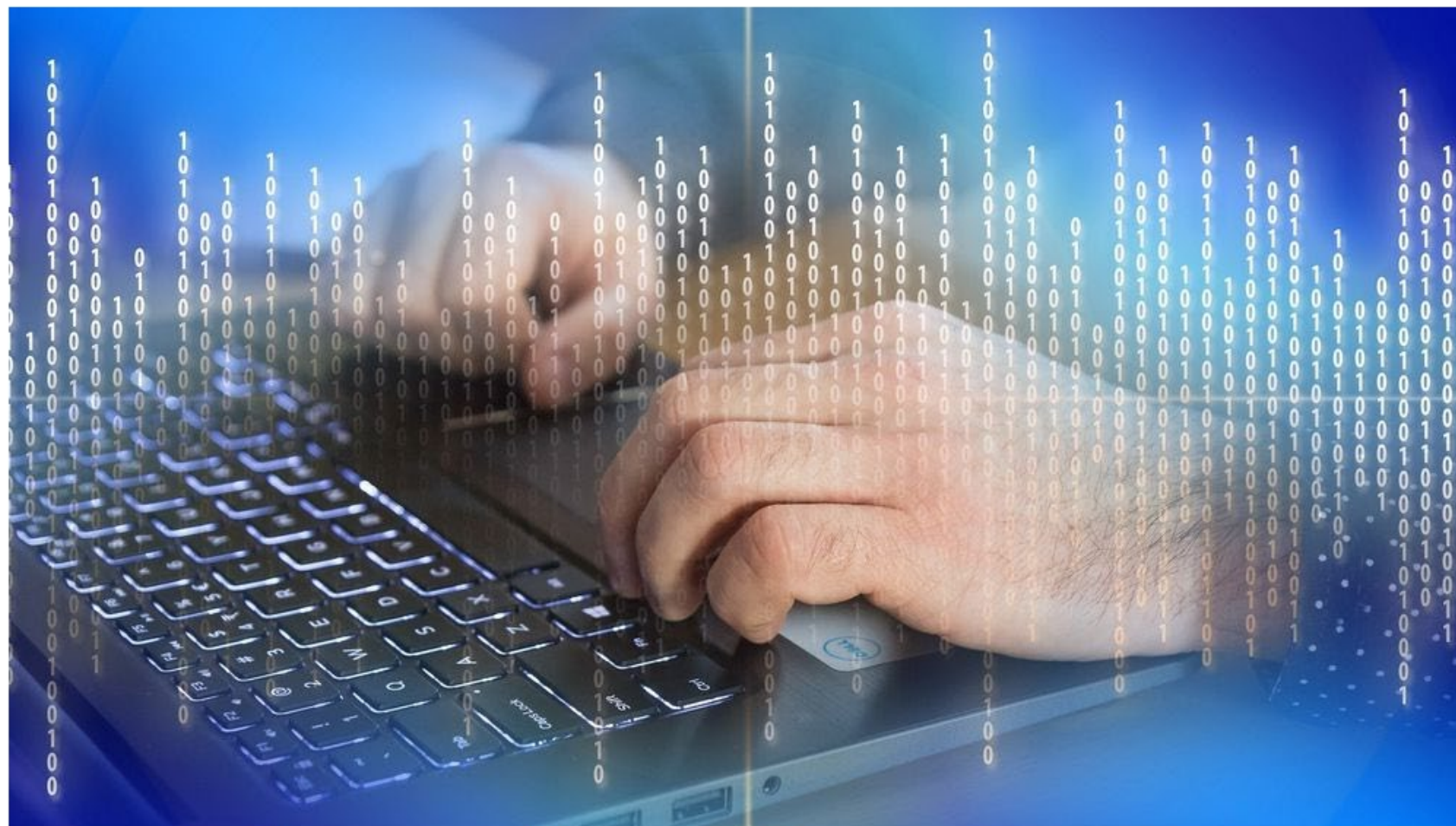
Det danske milliardkonsernet Vestas Wind Systems bekrefter at de er rammet av kryptovirus med krav om løsepenger. (Illustrasjonsfoto: Vestas)





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)





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.

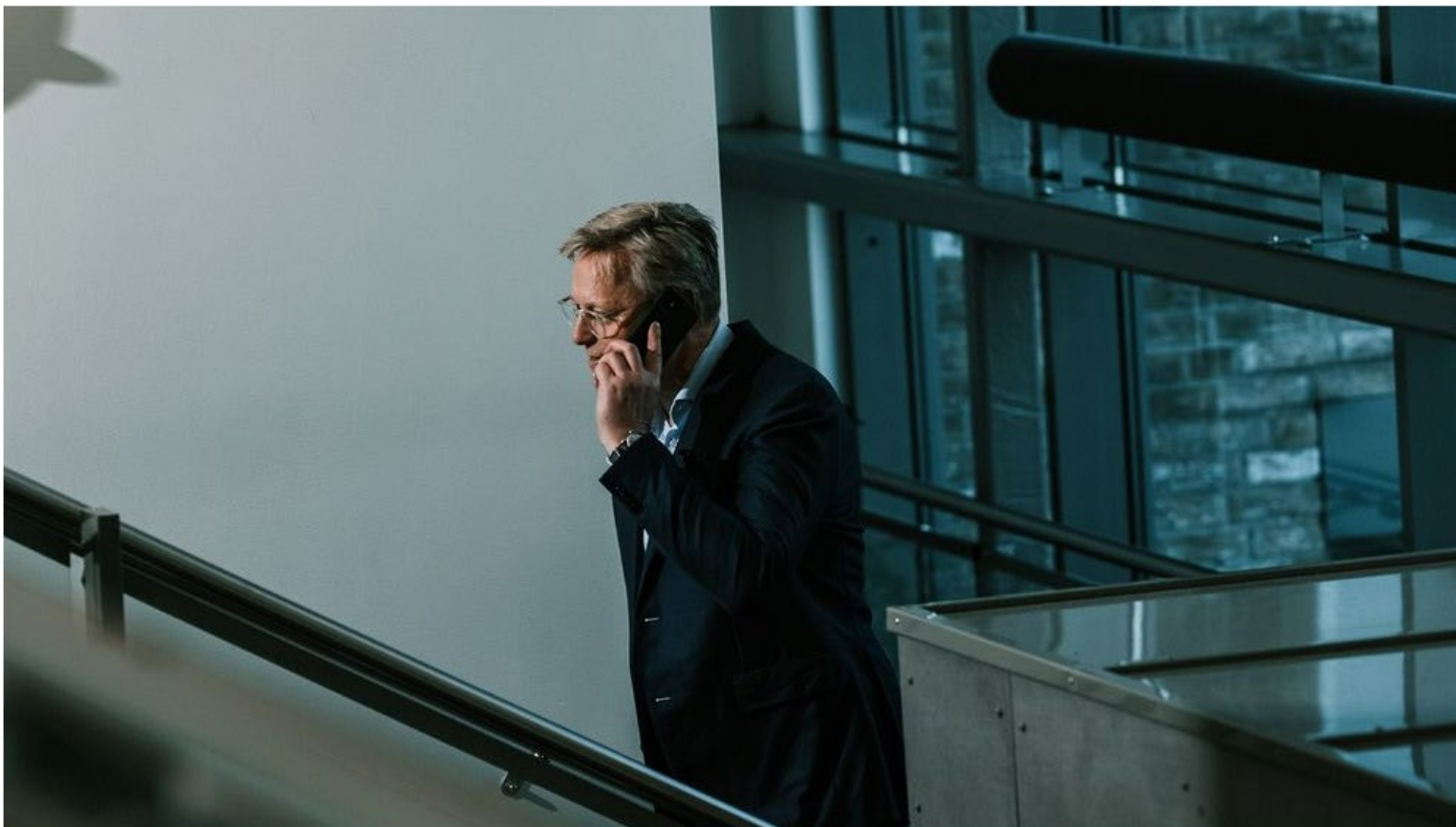


Nordic Choice Hotels er eid av Petter Stordalen.
© Adam Ihse/ TT NYHETSBYRÅN



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 stortilt svindelangrep som er i gang.



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

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

Svindelbølgen viser ingen tegn til å avta.

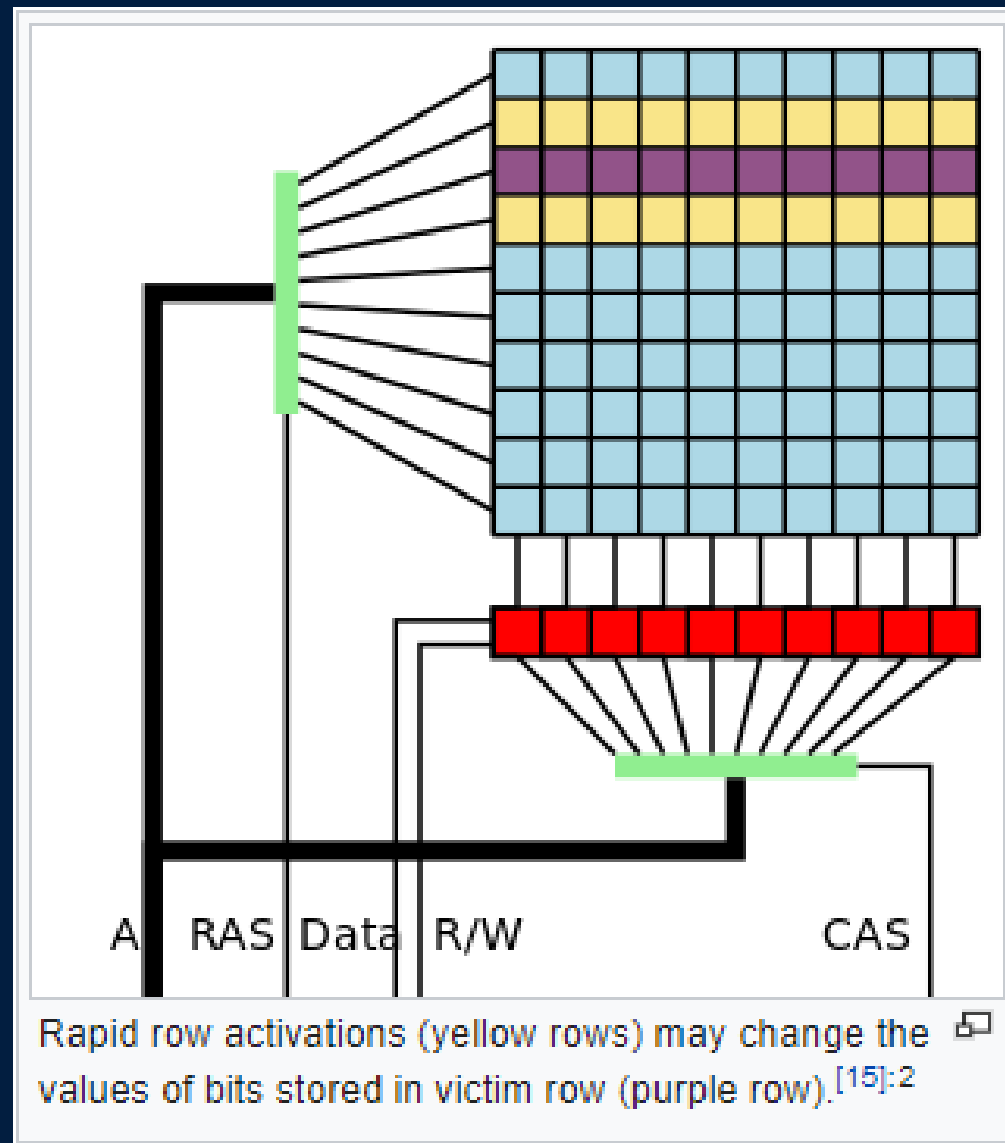


Flubot prøver typisk å lure mottakerne med påstand om talepost eller sporing av pakker. Kampanjen spres nå fra norske telefonnumre. (Foto: Are Thunes Samsonsen)



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.





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

Settings

Home


Find a setting

Update & Security

- Windows Update
- Delivery Optimization
- Windows Security

Windows Update

*Some settings are managed by your organization
[View configured update policies](#)

 You're up to date
Last checked: Today, 8:59 AM

[Check for updates](#)

[View optional updates](#)



Update of Mobile Operating System

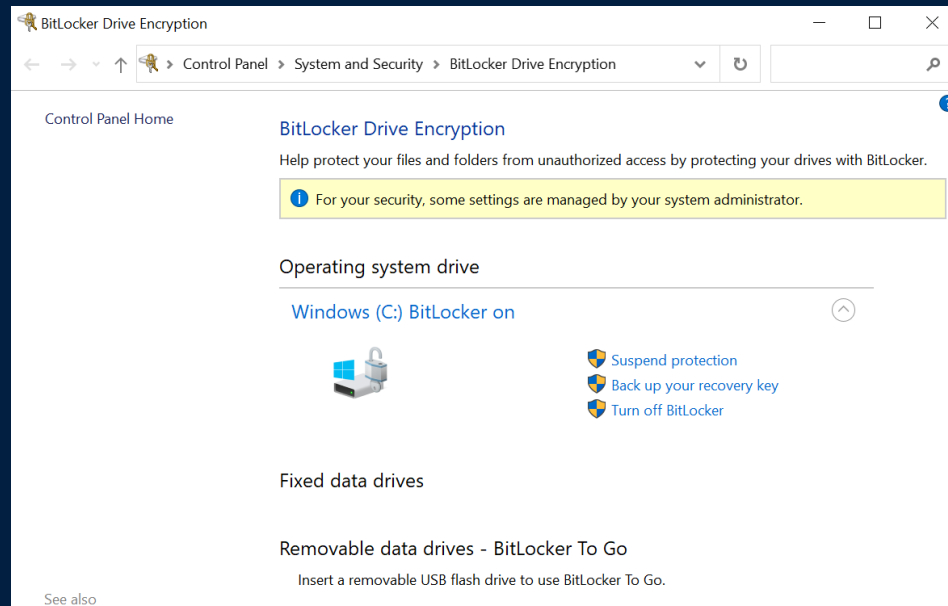
Turn on Automatic Updates on company devices





Bitlocker

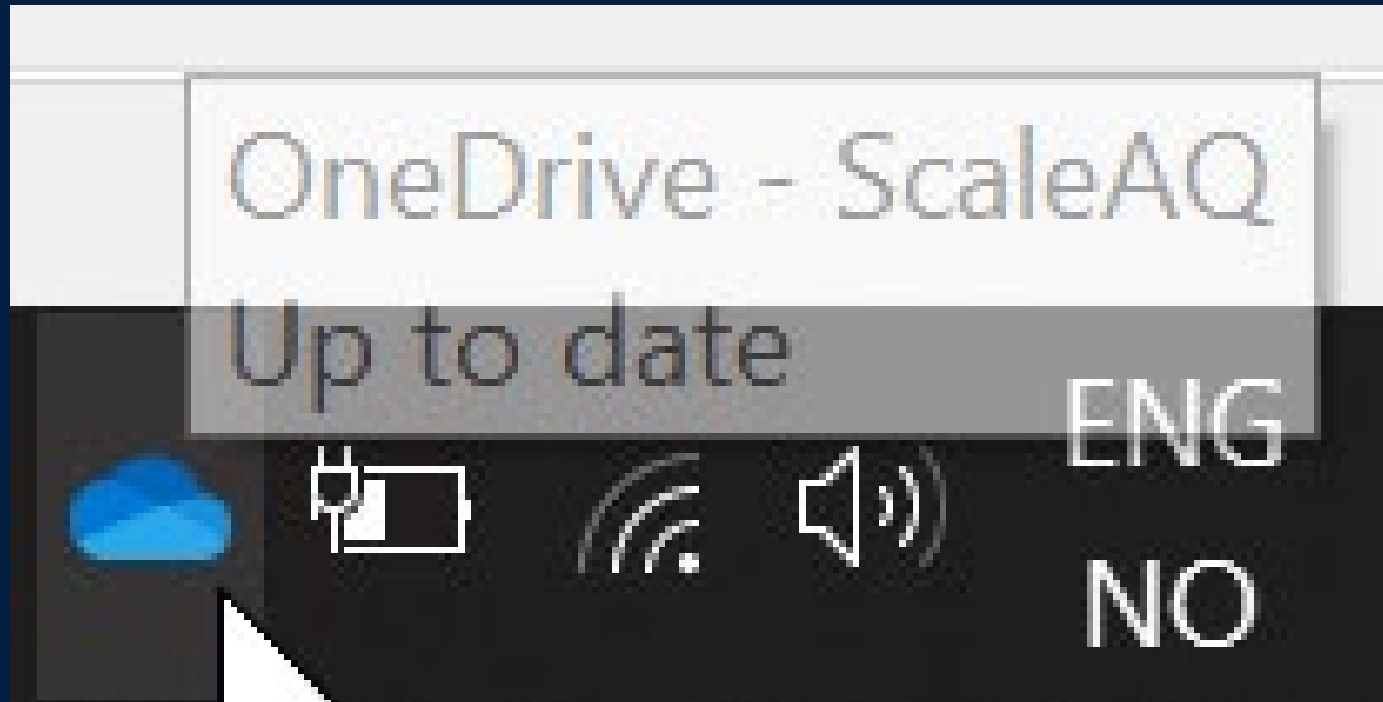
- All computers required to have the storage devices encrypted.
- This makes attacks harder and prevents access if device is stolen or lost.
- 140 computers unencrypted. Will be contacted with instructions shortly after this meeting.





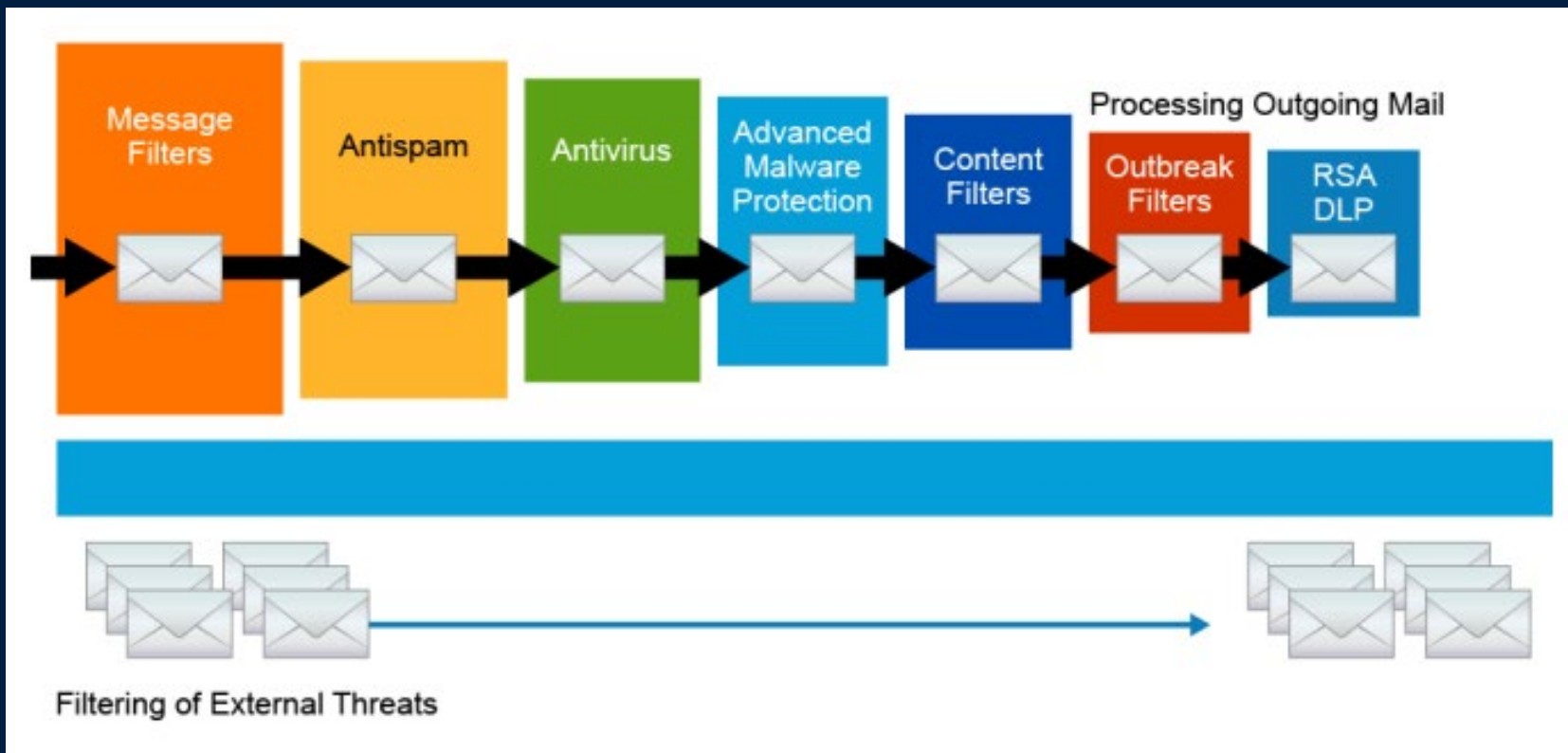
Use Sharepoint and OneDrive for your documents

- 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



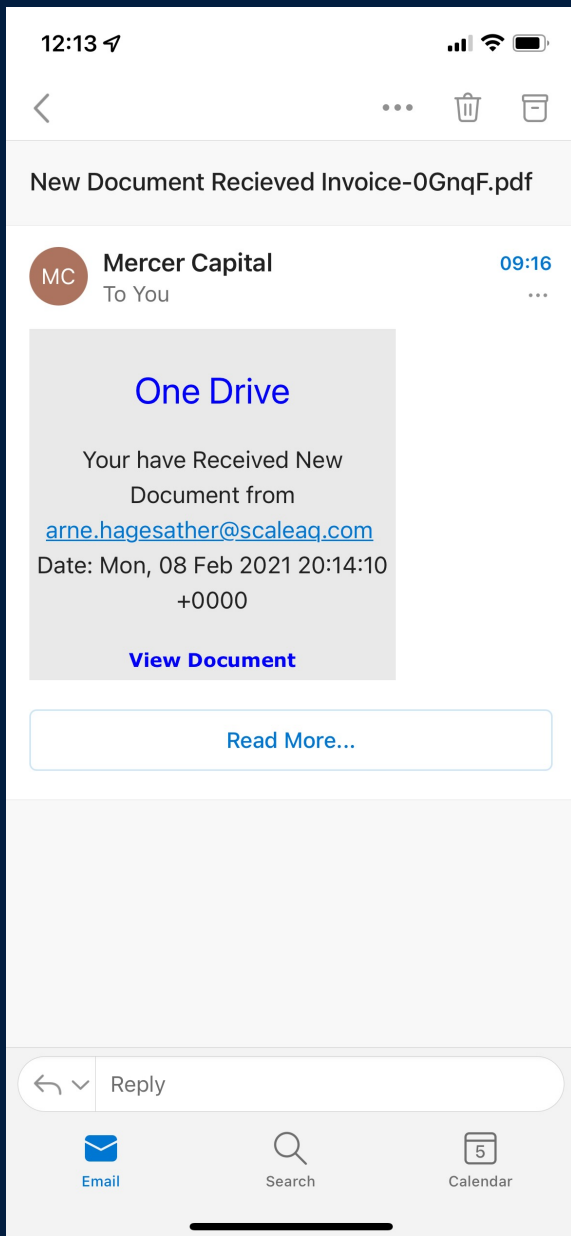


Still some emails delivered might be phishing

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



Phishing Test





Report Phishing

The screenshot shows an Outlook window titled "Sales order Data#DP00048537 Do-Gree Fashions Ltd. - Message (HTML)". The ribbon includes "File", "Message", "Help", and "Attachments". The "Report Message" dropdown menu is open, with the "Phishing" option selected. A tooltip for "Report phishing messages" is visible, stating: "Reporting helps Microsoft hone its filters to protect you from email designed to compromise your privacy and security." The email content includes a header from Tony Oliver to Arne Hagesaether, an attachment "SalesOrderData.Docx" (48 KB), and a body text that says "Please view the attached". At the bottom, there is contact information for Do-Gree Fashions Ltd. and logos for DO-GREE SOURCING, CTR, and CHAOS.

Sales order Data#DP00048537 Do-Gree Fashions Ltd. - Message (HTML)

File Message Help Attachments Tell me what you want to do

Delete Respond Share to Teams Quick Steps Move Tags Editing Immersive Translate Zoom SuperOffice Viva Insights

Sales order Data#DP00048537 Do-Gree Fashions Ltd.

Reply Reply All Forward

Tony Oliver <TonyOliver@dogree.com>
To Arne Hagesaether

SalesOrderData.Docx
48 KB

Please view the attached

Tony Oliver
Controller

Do-Gree Fashions Ltd.
7095 Robert-Joncas Place, Suite 225
Montreal, Quebec H4M 2Z2
Tel: 504 001 0000 Ext. 109

Mobile:504 001 0008

WWW.Dogree.com // WWW.Chaoshats.com

DO-GREE SOURCING CTR CHAOS

Report Message

- Junk
- Phishing
- Not Junk
- Options...
- Help

Report phishing messages
Reporting helps Microsoft hone its filters to protect you from email designed to compromise your privacy and security.



Phishing Training

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

You have 1 new training course(s) to complete - Message (HTML)

File Message Help Tell me what you want to do

Ignore Delete Archive Reply Reply All Forward Meeting IM Share to Teams Old Team Email Done Reply & Delete Create New Move OneNote Actions Assign Policy Mark Unread Categorize Follow Up Find Related Select Read Aloud Immersive Reader Translate Zoom Archive Search E-mail for sender


You have 1 new training course(s) to complete

SA Security and Compliance Team <trainingassignment@microsoft.com>
To Arne Hagesæther

📎 HOLD-Take training.ics
14 KB

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Microsoft 365



Arne Hagesæther, you have 1 training course(s) to complete that should take 7 min(s).

Please complete these by **December 13, 2021.**

[Go to training](#)

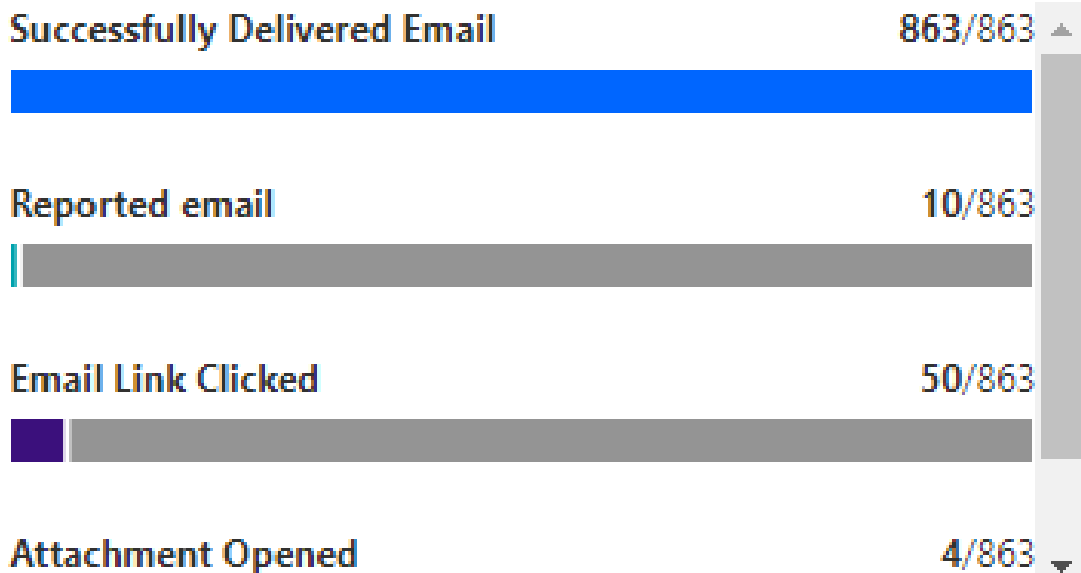
Hi Arne Hagesæther,



Phishing results

All user activity

4 of 863



Training completion

9 of 50 users completed training





Cisco Secure Endpoint protection

The screenshot displays the Cisco Secure Endpoint user interface. On the left is a navigation sidebar with the following elements:

- Secure Endpoint logo (a green play button icon)
- Secure Endpoint text
- Buttons: Scan Now, History, Settings
- Status: Connected (with a green checkmark icon)
- Scanned: 2021-11-28 10:14:46 PM
- Policy: Protect
- Isolation: Not Isolated
- CISCO SECURE logo
- [About](#) link

The main content area is titled "Scan" and shows a "Scan - Complete" notification. The scan results are as follows:

Files Scanned:	314284
Threats Detected:	0
Threats Removed:	0
Elapsed Time:	0:00:30:15

A message box with a green checkmark icon states: "Your scan has completed. There were no threats detected." Below this message is a "Scan History" button. At the bottom right of the interface is a "Close" button.



Umbrella Roaming Client

Umbrella Roaming Client (3.0.17.0)

IPv4 DNS status:

Protected

Encrypted

User Identity: SCALEAQ\ame.hagesather

IPv4 Address: 192.168.128.212

IPv6 DNS status:

Not Required

Unencrypted

User Identity:

IPv6 Address:

IP Layer Enforcement status:

Disabled

No Filters

Never Downloaded

Details:

Last Connected: less than a minute ago

Logging: Off

Client Name: SAQ-PC-685332

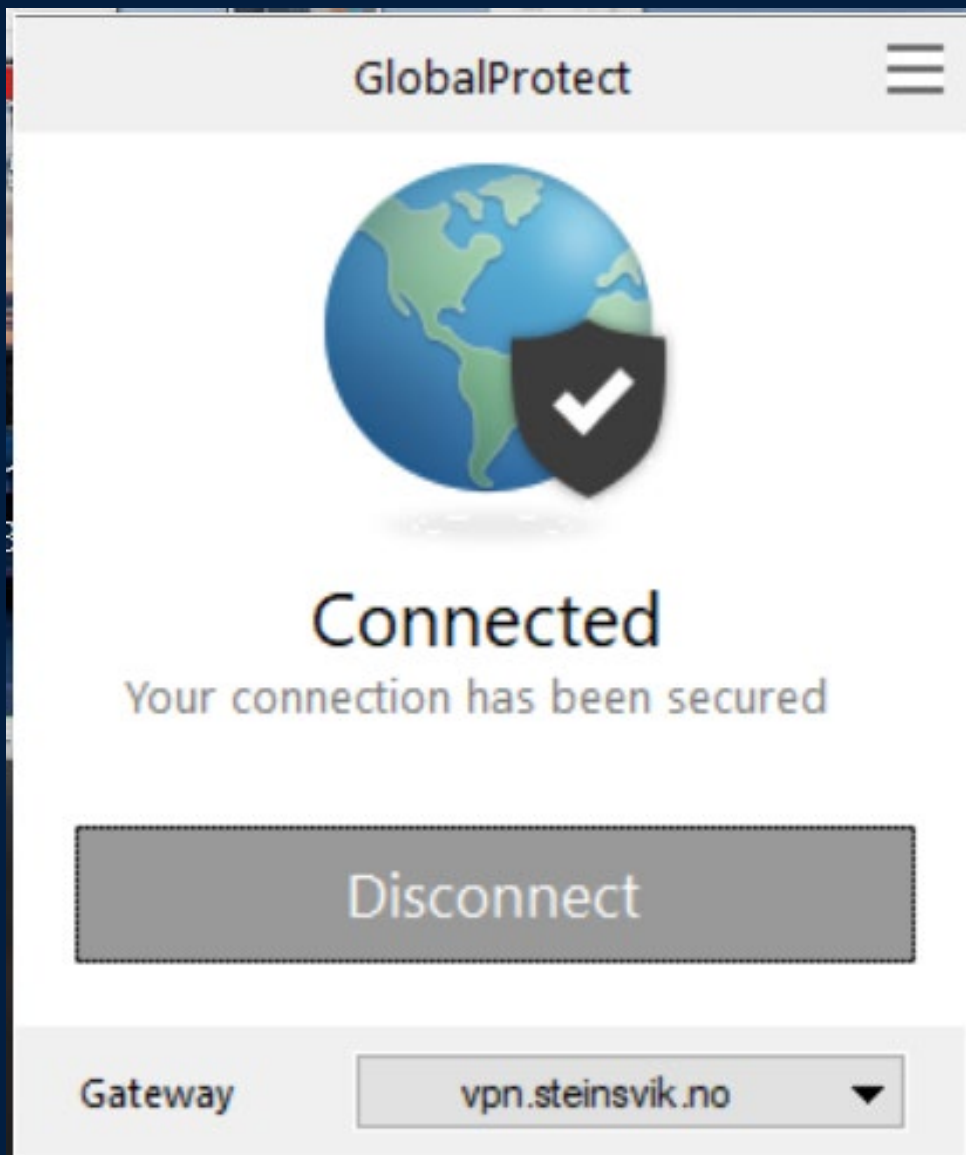
Organization Id: 2661076

Device Id: 010172361ECAEFCE

[Run Diagnostic Tool](#)



Use VPN when outside the Office





Umbrella Roaming Client works together with VPN

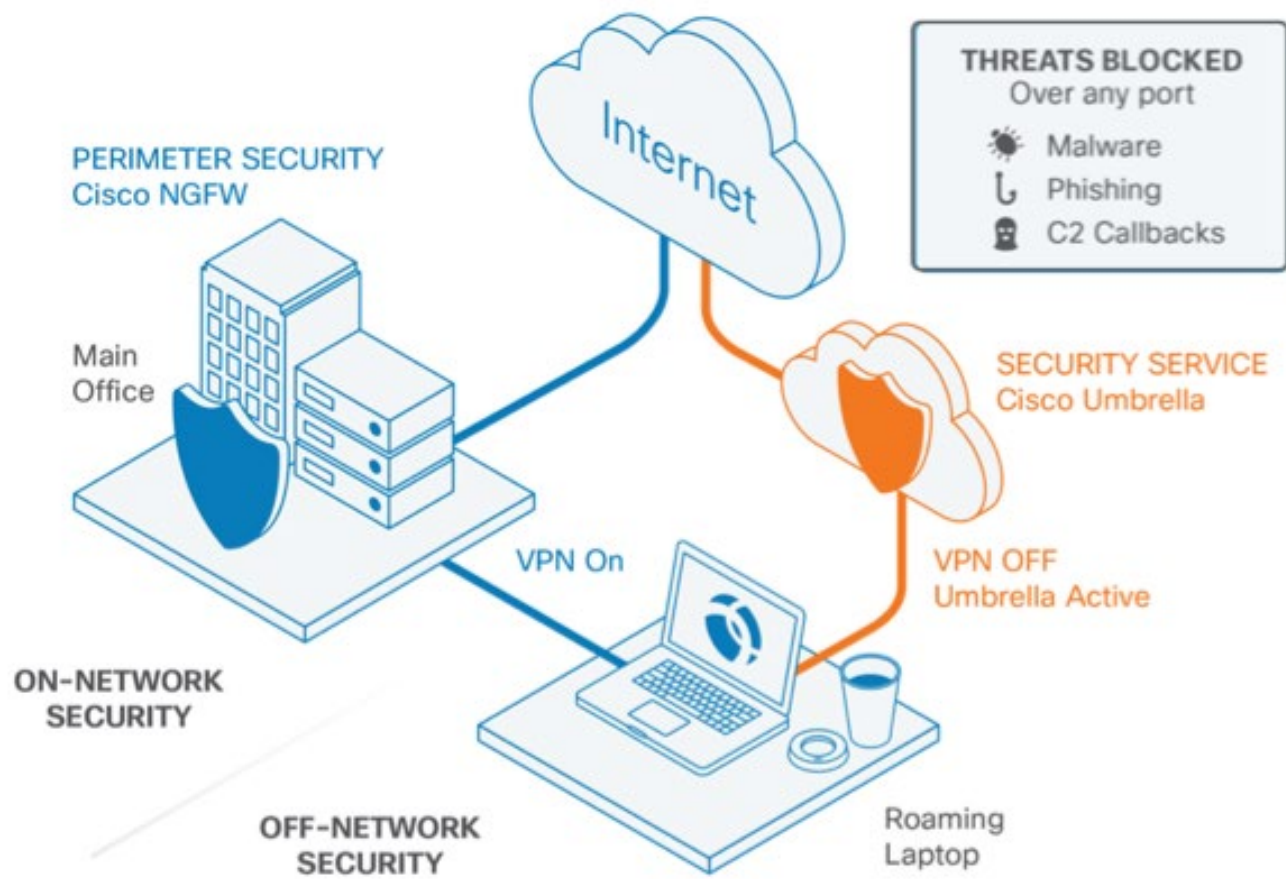


Figure 1: RC through the VPN — [Source](#)



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/>



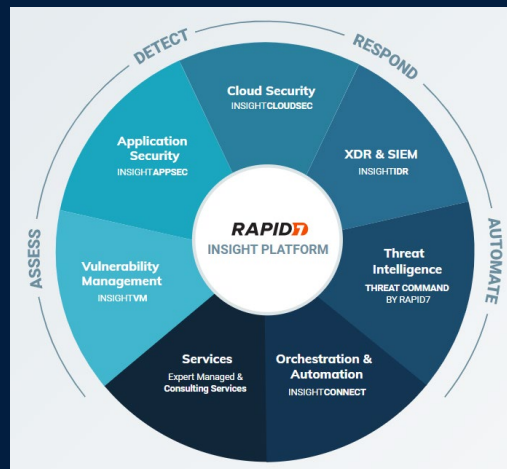
MFA – Multi Factor Authentication

- 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



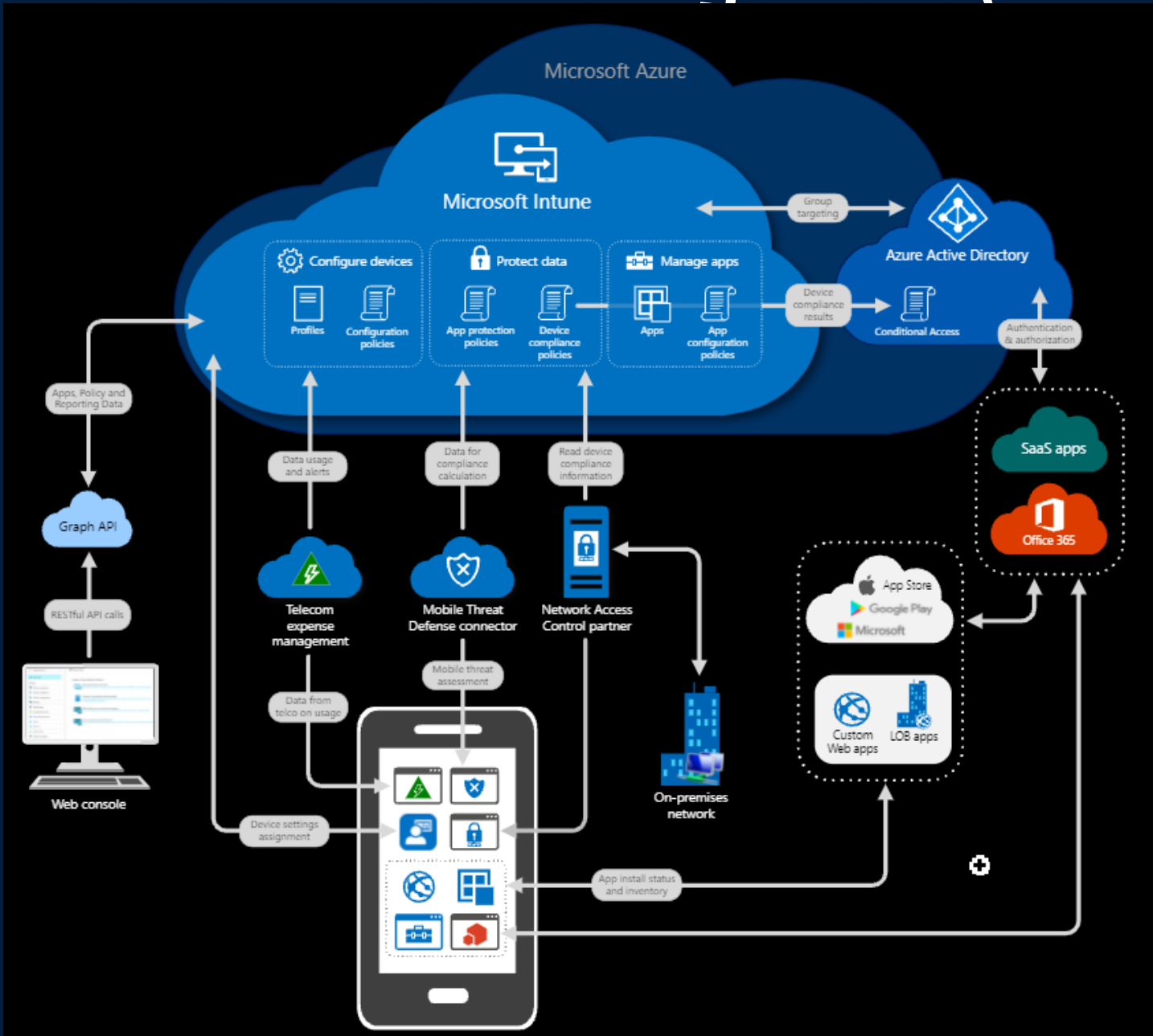


Mobile Device Management (TBA)

- 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 jailbroken 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

The screenshot shows a Microsoft Excel spreadsheet titled "FinancialReport" with a sensitivity label dropdown menu open. The menu options are: Public, General, Confidential, and Highly Confidential (which is selected and checked). A "Learn More..." link is also visible. The spreadsheet data is as follows:

	2017	2016	2015
Revenue	\$ 89,950.00	\$ 85,320.00	\$ 93,580.00
Gross margin	\$ 55,689.00	\$ 52,540.00	\$ 60,542.00
Operating income	\$ 22,326.00	\$ 20,182.00	\$ 18,161.00
Net income	\$ 21,204.00	\$ 16,798.00	\$ 12,193.00
Diluted earnings per share	\$ 2.71	\$ 2.10	\$ 1.48
Cash dividends declared per share	\$ 1.56	\$ 1.44	\$ 1.24
Cash, cash equivalents, and short-term investments	\$ 132,981.00	\$ 113,240.00	\$ 96,526.00
Total assets	\$ 241,086.00	\$ 193,468.00	\$ 174,303.00
Long-term obligations	\$ 104,165.00	\$ 62,114.00	\$ 44,574.00
Stockholders' equity	\$ 72,394.00	\$ 71,997.00	\$ 80,083.00

The status bar at the bottom of the Excel window shows "Ready" and "Highly Confidential" with a lock icon, both highlighted in yellow.



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**.



S 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 ruterer 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.



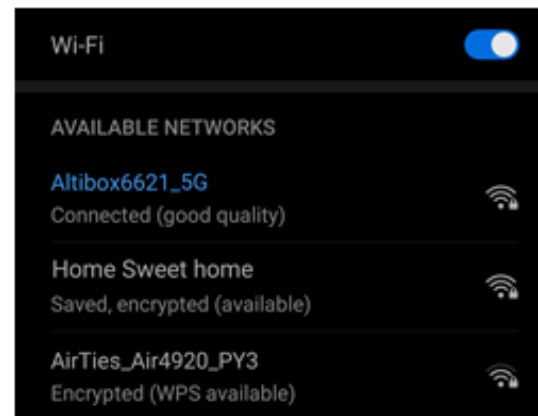


Protect your home network

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 internettleverandøren 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.





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

The screenshot shows the Helsenorge.no website interface. At the top, the browser address bar displays "helsenorge.no". The website header includes the logo "HELSE NORGE", a menu icon labeled "meny", and a search icon labeled "søk". On the right side of the header, there is a teal button labeled "Logg inn" with a lock icon. A prominent yellow warning box is centered on the page, containing a warning icon (a triangle with an exclamation mark) and the following text: "Advarsel: Ikke klikk på lenker i e-poster om varsel om ny melding fra helsenorge.no. Det sendes for tiden ut falske e-poster som utgir seg for å være fra Helsenorge. Hvis du har mottatt e-post med varsel om ny melding fra prøvesvartjenesten, må du ikke klikke på lenkene i den. Helsenorge ber deg aldri om kredittkortinformasjon eller passord og koder i en henvendelse. Har du oppgitt kort- eller kontoinformasjon, sperr kort og kontoer umiddelbart." A close button (an 'X' in a square) is located in the top right corner of the warning box.



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 😊