Be aware that <u>you</u> are the business model of free online services

DON'TS:

☒ Do not open attachments send via e-mail without first scanning it for virus, malware, spyware, Trojans etc. – even if you know the sender.

☒ Do not plug-in third-party USBs into work computers without first checking with your IT dep't.

☒ Do not connect to any and all public WI-FI

☒ Do not install mobile applications or software from untrusted sources

Additional online resources

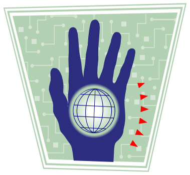
Guidance on setting up two-factor authentication on popular online media and services, see https://www.theverge.com/2017/6/17/15772142/how-to-set-up-two-factor-authentication

6 steps to Better Security

www.lockdownyourlogin.org

STOP.THINK.CONNECT campaign and materials

www.stopthinkconnect.org

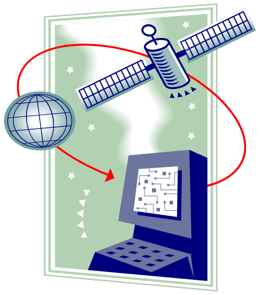


Stay safe online

Vigilantia Diligentia Animus

Veiligheidsdienst
Aruba

Basic Cyber Security Hygiene



For Technical & Non-Technical Readers

For Technical Readers

- Identify hardware and software in the network.
- Be better prepared against data leaks, intellectual property theft, espionage, financial crime by identifying the "crown jewels of information processes"
  - ⇒ establish data management (information rights management) policies;
  - ⇒ restrict access to confidential / sensitive data to only those employees who need to work with them;
  - ⇒ Review, revoke and renew access policies.
- Patch systems and automated processes – update your systems periodically to make sure the latest security patches are in place.
- Establish clear policies and procedures for employee use of your organization's information technologies.
- Risk-driven approach; identify the potential risks to your company & how to mitigate these
- Provide awareness sessions (technical and non-technical) for and together with employees at all levels.
- Consider email alias policies that don't give out employee's full names.
- Back-up or copy sensitive and critical information and databases.

Perform structurally

- ♦ Monitor, log, analyze, and report successful and attempted intrusions to your systems and networks.
- ♦ Have a continuity plan if a breach should happen in order to quickly recover to normal or basic operation functionality.
- ♦ Use adequate data encryption where possible and include procurement requirements for future services and systems.
- ♦ Use unique passwords across your services and devices (enhanced by a password manager).
- ♦ Limit remote access.
- ♦ If you need to work on a device away from the office;
  - ⇒ Use a privacy screen to prevent shoulder surfing.
  - ⇒ Store your laptop in a secure way, e.g. a safe.
- ♦ Be knowledgeable of your "zorgplichten" (Care obligations).
- ♦ Identify new or changes in information infrastructure dependencies and its effects in responsibilities.

Additional reading

Framework for Improving Critical Infrastructure Cybersecurity (www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf)

Holistic Management Of Employee Risk (HoMER) (www.cpni.gov.uk/system/files/documents/da/00/Holistic-Management-of-Employee-Risk-HoMER-Executive-summary.pdf)

STOP.THINK.CONNECT (www.stopthinkconnect.org)

Review of Cyber Hygiene practices (www.enisa.europa.eu/publications/cyber-hygiene)

Cyber Hygiene posters (www.enisa.europa.eu/media/multimedia/posters/cybersecurity-education-posters-2016/enisa-eduposters-en.pdf)

For Non-Technical Readers

Prevent online traces while surfing and working on the internet

DO's:

- * Enable two-factor authentication password when possible
- * Use anti-virus to check external drives (e.g. USB) before opening files on work computers
- * Make sure you update your or automate your operating system
- * Keep a clean machine – make sure you keep all your software and internet-connected devices up-to-date to reduce the risk of malware infection .
- * Own your online presence – limit how much information you share on social media. Check your privacy and security settings regularly.
- * Lock your screen when leaving your computer
- * Consider using a paid Virtual Private Network (VPN) for enhanced secured connections
- * Use unique passwords across services and devices (supported by a password manager)