Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Finance FDF
General Secretariat

National Cybersecurity Centre NCSC
www.ncsc.admin.ch

NCSC

Home Office:

End User Guideline

Introduction

Following the document "Home Office: Secure Remote Access", we would like to provide a brief information for the end user on how to better protect his own environment and thus also reduce the risk for the employer.

Recommendations

Accessing the Computer

- Protect the access to your work computer with a **strong password**. If your company uses **2-factor authentication** for company equipment, do not leave the smartcard/dongle plugged in when you leave your home, but keep it separate and safe.
- If you are working with a **BYOD** ("Bring Your Own Device"), please adjust the security settings accordingly. If in doubt, ask your IT department or the responsible person for a brief instruction.
- Use a password protected **screen saver**, which activates after 15 minutes of inactivity at the latest.
- Use a **password manager** to save your passwords. Either the solution provided by your employer or an offline password manager such as KeePass (https://keepass.info/)
- Check whether **disk encryption** is active on your work computer. If you are unsure, ask your IT department.
- If you connect your work computer to your **home network**, make sure you do not make it visible to other computers on the network. If you need to add it to your home group for some reasons, make sure the option to share files is turned off.

Securing the Connections

- Make sure that you have access to your company's infrastructure and can dial in via the **VPN/ remote access** of your company.
- **Secure** your **Wi-Fi** at home with a strong password, always use WPA2 or - if available on your Wi-Fi device - WPA3.
- Access to the administration interface of your home router should also be protected by a (strong) password. Make sure that you have changed the default password. You should find a guideline or a manual for doing so on the manufacturer's website of your router model.

- Make sure that your home **router** always has an **up-to-date version** of the firmware.
- If your normal internet traffic is not sent through the company network, you have less protection. So be more careful when surfing / emailing. If all your traffic goes through the company network (via a VPN/Remote Access), you should avoid YouTube/ streaming on this device in order to save bandwidth.

Data Security

- Do **not** use **private cloud services** for storing business documents.
- Do not mix private and business data. If you work with your own device, create an encrypted container for the business data, e.g. by encrypting a USB stick or encrypt the entire hard disk using Bitlocker[1].
- Make sure that you **back-up** all your locally stored data. Use two different disks or USB sticks and keep them safe. Make sure that the medium does not stay connected to the computer, but is always ejected when the backup is complete.

Physical Security

- If you need to leave your home, make sure that your electronic devices are either switched off or locked - including any mobile phones you might use to check email or make phone calls for work.
- If you live in a **multi-person household**, especially with young children, you should lock your computer even if you are only away from the workplace for a short time to prevent accidental tampering.
- If you cannot set up a **separate workplace** in your home, you should store your devices in a safe place where they are no longer visible at the end of your working day. This not only reduces the likelihood from them being opened or stolen, but also makes it easier to keep your work and personal life separate.

Separate work from home use

- Do not pay your bills at home on the same computer that you use for working. Not only can you create confusion for yourself, but you could compromise your personal information as well if a cybercriminal has successfully attacked your company and vice versa.
- Do not send work-related emails from your private email address and vice versa.
- Speaking of **home schooling**, it is important to keep your child's digital curriculum / activities separate from the device you use for company work.

[1] https://www.windowscentral.com/how-use-bitlocker-encryption-windows-10

- Never let anyone in your household access your work computer, even if you are sitting next to it.

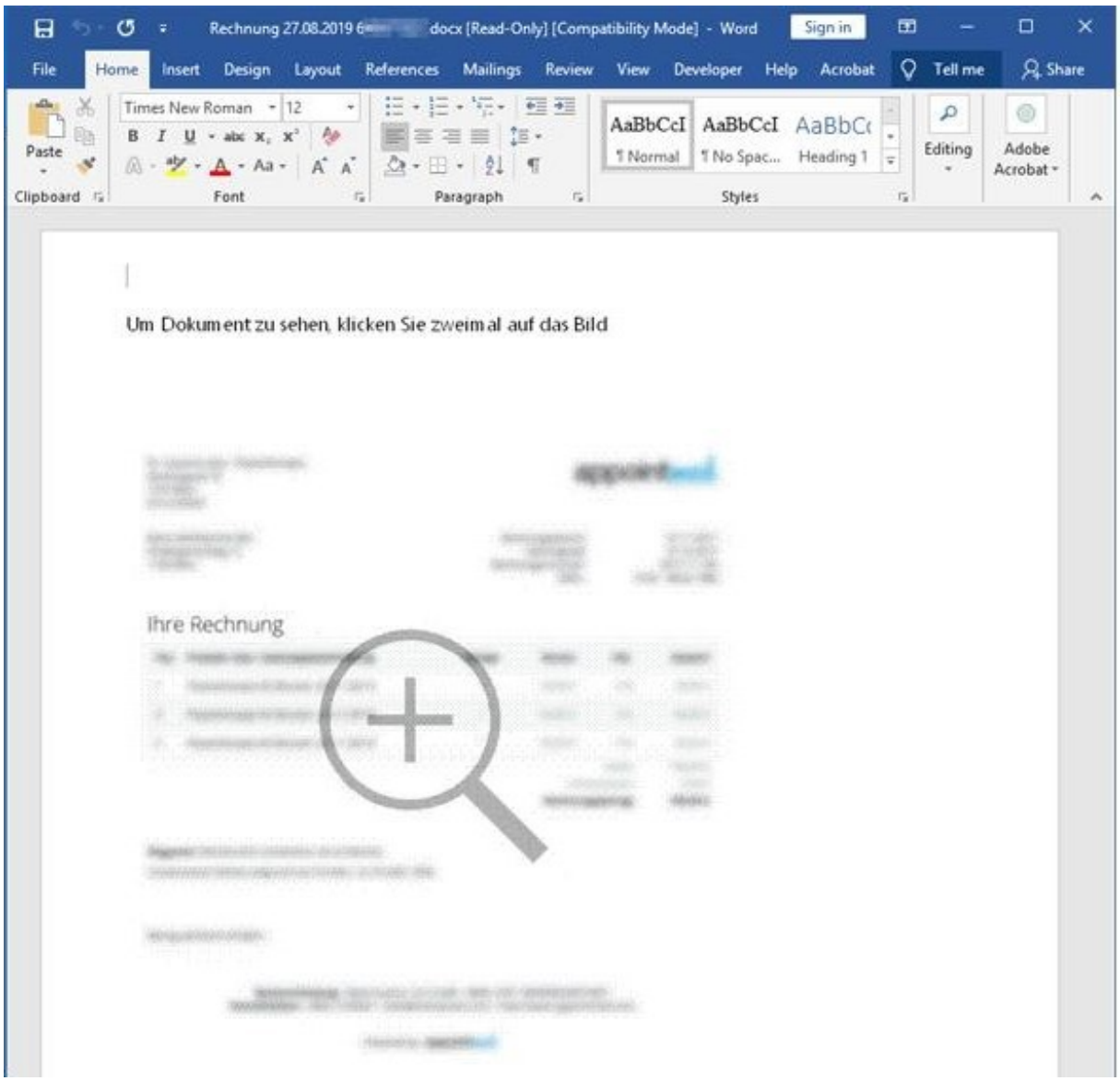
Notes about Cyber Security

- If you need to download **programs** or **software** from the **Internet**, be sure that you actually are on the manufacturer's website and do not download any malware (attackers like to pretend being well-known companies or authorities[2]). This applies especially if you download collaboration software for home office use (e.g. conference software).
- **Phishing emails**: Many attackers try to capitalize on current events and the public attention they create (a typical example is the Corona / Covid-19 crisis), and pretend having information, propose advice or want to ask questions about the subject. Check such e-mails with a sharp eye and do not open attachments unless they come from a verified trusted source known to you. Pay special attention to emails masquerading as high-ranking employees and pay close attention to the actual email address of the sender. Please note that sender addresses in emails may be forged and the real address is only visible in the email header.[3]
- In case of doubt, always ask the sender directly (ideally by telephone or in a text chat)
- If in doubt or if you have already opened a suspicious document, contact your helpdesk / IT department or the responsible person promptly.
- You may report phishing emails or emails with attachments at https://www.antiphishing.ch. Please note that these messages are processed automatically and you will not receive any feedback. If you wish to report a case and need feedback, please contact the National Contact Point via the reporting form (https://www.report.ncsc.admin.ch/en/)
- **Never enable macros** and never ignore security warnings when you open a document that has been sent by email or that you have downloaded from the Internet. If in doubt, do not open the document and call the sender or contact your IT department.

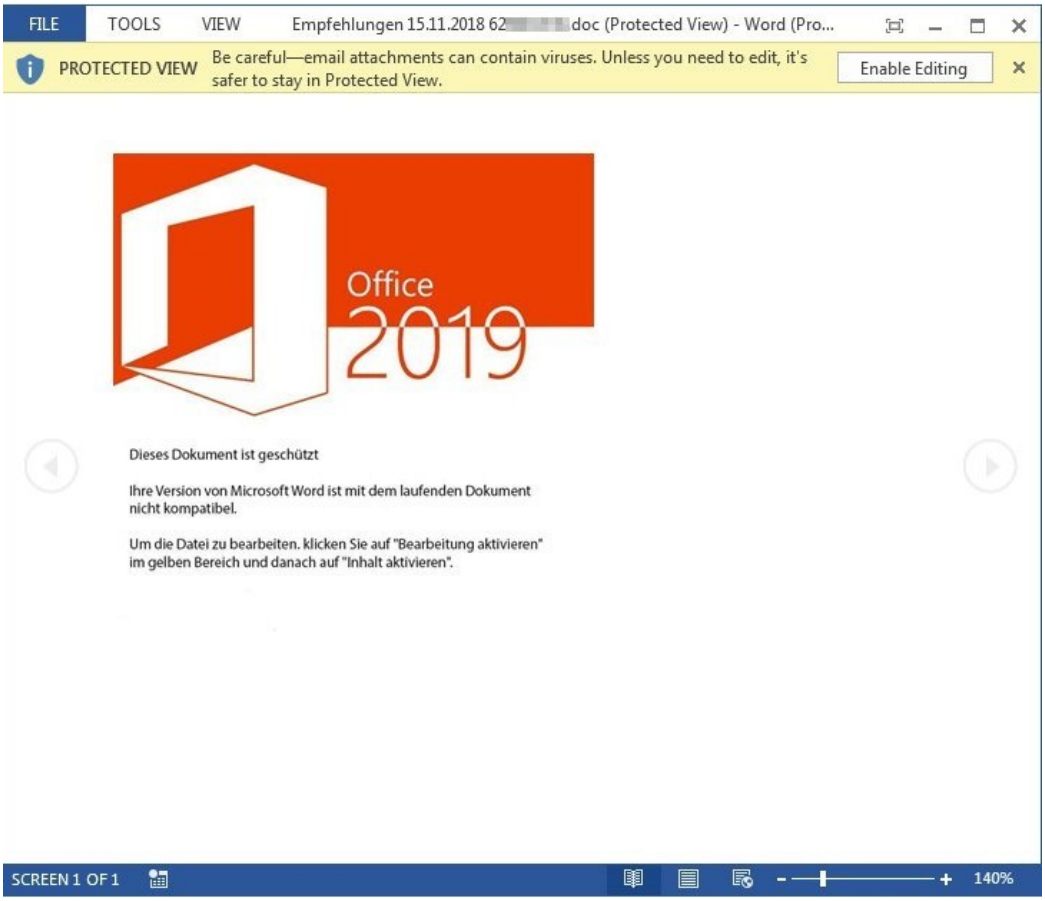
  Below, screenshots 1 and 2 show examples of Word attachments with macros.

[2] https://www.ncsc.admin.ch/ncsc/de/home/aktuell/news/news-archiv/zunehmender-missbrauch-der-namen-von-bundesstellen-und-firmen.html (only German, French or Italian)

[3] https://www.howtogeek.com/121532/htg-explains-how-scammers-forge-email-addresses-and-how-you-can-tell/



Screenshot 1: Double-clicking the image runs macros and infects your PC with malware.



Screenshot 2: Clicking "Enable Editing" executes the macros and infects you with malware.

If you have questions about this document please contact outreach[at]ncsc.ch.