Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Secrétariat général

Centre national pour la cybersécurité NCSC
www.ncsc.admin.ch

NCSC

Télétravail:

recommandations pour l'utilisateur

Introduction

En tant que complément au document "Télétravail: Sécuriser son accès à distance", nous souhaitons mettre à disposition une information plus brève à destination des utilisateurs finaux. Celle-ci leur permettra de mieux protéger leur infrastructure, et ainsi également réduire le risque pour leur employeur.

Recommandations

Accès au système

- L'accès à votre ordinateur doit dans tous les cas être protégé par un **mot de passe** robuste. Si votre employeur prévoit un deuxième facteur d'authentification pour ses appareils, ne laissez par la smartcard ou la clé USB insérée lorsque vous quittez la pièce, mais conservez-les séparément.
- Si vous travaillez avec un appareil **BYOD** („Bring Your Own Device“, votre propre appareil, n'étant pas fourni par l'employeur), adaptez les mesures de sécurité en conséquence. En cas de nécessité, demandez conseil à la personne ou l'unité en charge de l'informatique.
- Utilisez un **écran de veille** avec mot de passe, s'affichant après 15 minutes d'inactivité au maximum.
- Utilisez un **gestionnaire de mot de passe**. Qu'il s'agisse de la solution proposée par votre employeur ou un gestionnaire (dans l'idéal) hors ligne tel que KeePass (https://keepass.info/).
- Vérifiez que le **chiffrement de votre stockage de données** est activé sur votre poste de travail. En cas de doute, demandez à la personne ou l'unité en charge de l'informatique.
- Lorsque vous connectez votre ordinateur professionnel à votre **réseau privé**, assurez-vous que l'appareil n'est pas visible par d'autres appareils sur le réseau. Si vous devez l'intégrer au groupe résidentiel, assurez-vous que l'option "partage de fichiers" soit désactivée.

Connexions sécurisées

- Assurez-vous d'avoir accès à l'infrastructure de votre employeur et de pouvoir vous connecter à travers le **VPN/l'accès à distance** fourni par votre employeur.

- Protégez votre accès Wi-Fi par un **mot de passe robuste**, utilisez toujours WPA2, ou même WPA3 si celui-ci est supporté par votre appareil.
- L'accès aux paramètres de votre routeur devrait aussi être protégé par un mot de passe. Veillez à modifier le mot de passe standard. Des informations à ce sujet doivent être disponibles sur le site web du fournisseur.
- Assurez-vous de toujours utiliser la **dernière version logicielle** pour votre routeur.
- Si votre trafic Internet normal ne passe pas à travers le réseau de votre employeur, la protection est moindre. Soyez donc plus prudent lorsque vous naviguez/envoyez des e-mails. Si tout le trafic passe par un réseau professionnel (par un VPN) il convient d'utiliser la bande passante avec parcimonie et de renoncer à des activités exigeantes à ce niveau comme le streaming/YouTube

Sécurité des données

- **Renoncez** à l'utilisation de **services cloud privés** pour sauvegarder des documents professionnels.
- **Ne mélangez pas** les **données privées** et **professionnelles**. Si vous travaillez avec votre propre appareil, prévoyez un container chiffré pour les documents professionnels (p.ex. une clef USB chiffrée ou un chiffrement du disque dur par Bitlocker[1].
- Veillez à effectuer une **sauvegarde** (backup) de vos données enregistrées localement. Utilisez deux clefs USB ou disques distincts et conservez-les en lieu sûr. Le support de la sauvegarde ne doit pas rester connecté à l'appareil mais doit toujours être retiré après l'opération.

Sécurité physique et télétravail

- Lorsque vous devez quitter votre appartement, assurez-vous que vos **appareils** soient **éteints** ou **bloqués**, y compris les téléphones portables que vous utilisez pour traiter des e-mails ou passer des appels professionnels.
- Si vous **vivez avec d'autres personnes**, en particulier de petits enfants, il convient de bloquer l'ordinateur même si vous vous absentez brièvement, afin d'éviter des manipulations non désirées.
- Si vous ne pouvez pas organiser de **place de travail séparée** à la maison, il convient de conserver vos appareils en lieu sûr après votre journée de travail, à l'abri des regards. Cela permet d'éviter qu'ils soient ouverts ou volés, mais également d'assurer une séparation entre vie privée et vie professionnelle.

[1] https://support.microsoft.com/fr-ch/help/4028713/windows-10-turn-on-device-encryption; https://www.windowscentral.com/how-use-bitlocker-encryption-windows-10 (en anglais)

Séparer les appareils professionnels des appareils privés

- Ne payez pas vos factures sur la même machine que celle utilisée pour votre travail. Vous pouvez non seulement générer de la confusion, mais aussi compromettre vos données personnelles si un criminel cherche à pénétrer le réseau de votre employeur, et inversement.
- N'envoyez pas d'e-mail de nature professionnelle depuis votre adresse privée, et inversement.
- Au sujet de **l'enseignement à domicile**: il est important de ne pas suivre le plan d'étude de vos enfants depuis votre appareil professionnel.
- Ne laissez personne à la maison accéder à votre ordinateur professionnel, même lorsque vous êtes assis à côté.

Cybersécurité en général

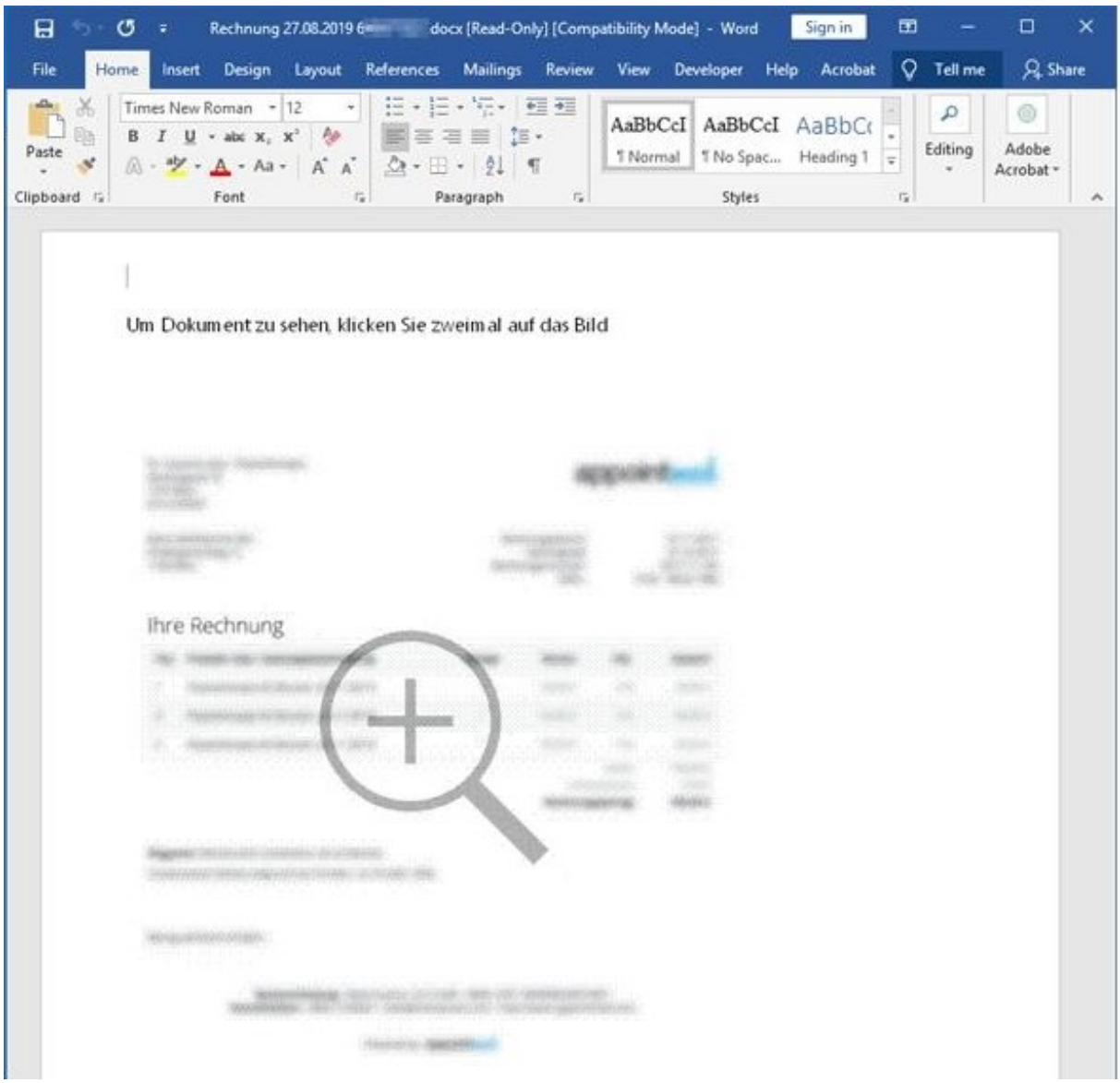
- Si vous devez **télécharger** des **logiciels** depuis **Internet**, assurez-vous de le faire depuis le site officiel du fournisseur et de ne pas installer un logiciel malveillant (les attaquants usurpent volontiers les identités d'entreprises ou autorités connues[2]). Cela vaut en particulier pour les téléchargements effectués en vue d'une activité de télétravail (p.ex. logiciels de web conférence)
- **E-mails de phishing**: de nombreux attaquants cherchent à tirer profit d'évènements actuels et de l'attention qu'ils suscitent (un exemple typique est la crise du coronavirus), et prétendent détenir des informations, proposer des conseils ou vouloir poser des questions à ce sujet. Soyez toujours méfiants envers ce genre d'e-mails et n'ouvrez pas de pièce jointe, à moins qu'il s'agisse d'une source connue et en laquelle vous avez pleine confiance. Méfiez-vous en particulier des e-mails semblant venir de collaborateurs de la hiérarchie supérieure (p.ex. le CEO), et prêtez attention à l'adresse véritable de l'expéditeur. L'adresse d'expéditeur peut être falsifiée et la véritable adresse n'est visible que dans l'en-tête (header) de l'e-mail.[3]
- En cas de doute, demandez directement à l'expéditeur affiché si l'e-mail vient bien de lui (par téléphone idéalement).
- Vous pouvez également vous adresser à votre Helpdesk ou auprès de la personne ou service en charge de l'informatique.
- Vous pouvez annoncer des e-mails de phishing ou contenant des pièces jointes suspectes sur https://www.antiphishing.ch. Nous vous précisons que les annonces sont traitées automatiquement et que vous ne recevrez pas de réponse. Si vous

[2] https://www.ncsc.admin.ch/ncsc/de/home/aktuell/news/news-archiv/zunehmender-missbrauch-der-namen-von-bundesstellen-und-firmen.html

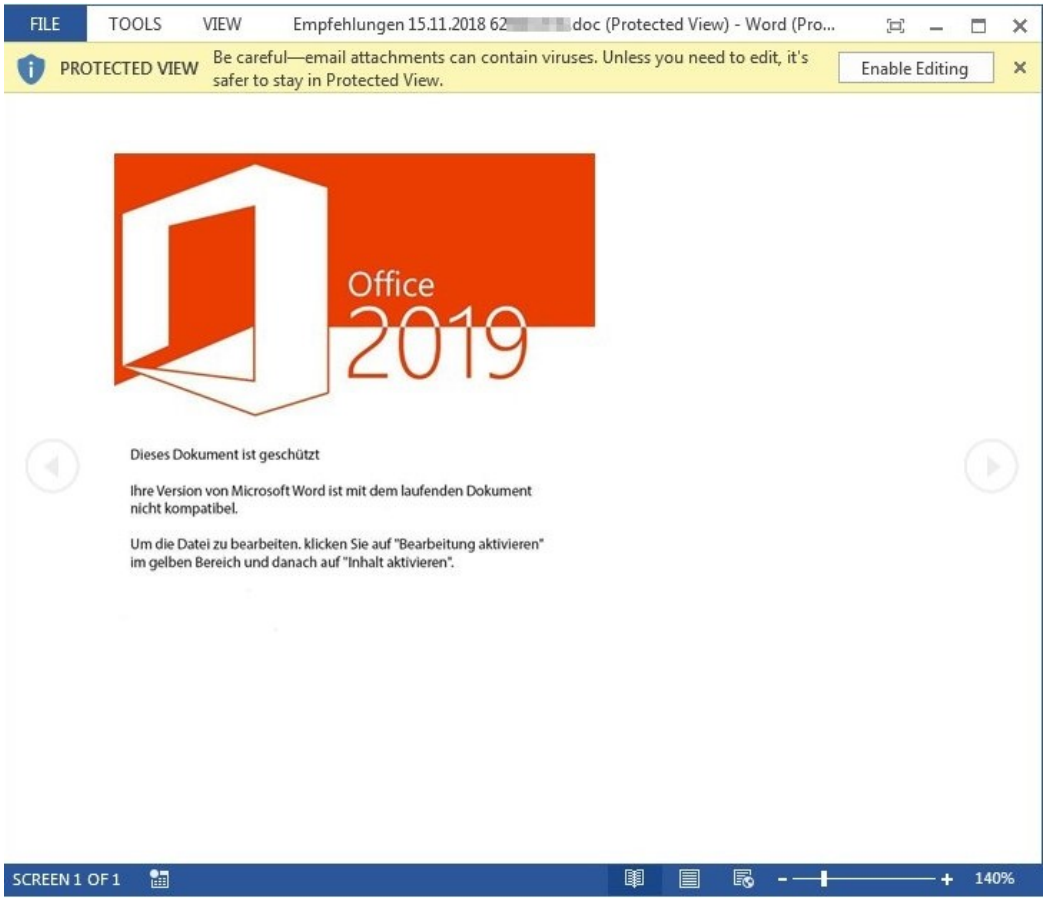
[3] https://www.howtogeek.com/121532/htg-explains-how-scammers-forge-email-addresses-and-how-you-can-tell/ (en anglais)

souhaitez annoncer un incident et avez besoin d'un retour, veuillez-vous adresser au Centre national pour la cybersécurité, par formulaire d'annonce (https://www.report.ncsc.admin.ch/fr/).

- **N'activez** pas les **macros** et n'ignorez jamais les alertes affichées lorsque vous ouvrez un document vous ayant été envoyé par e-mail ou téléchargé sur Internet. En cas de doute, renoncez à ouvrir le document et prenez contact téléphoniquement avec l'expéditeur ou avec la personne ou service en charge de l'informatique. Ci-dessous, des exemples de pièces jointes Word avec macros.



Capture d'écran 1: Avec un double clic sur l'image, les macros sont exécutées et la machine infectée avec un maliciel.



Capture d'écran 2: En appuyant sur «Enable Editing» ou «activer la modification», les macros sont exécutées et la machine infectée avec un maliciel.

Pour toute question sur le document, veuillez-vous adresser à outreach[at]ncsc.ch.