

Considérations relatives aux appareils



Présentation et considérations	Considérations techniques	L'utilisation sécuritaire des outils de collaboration	Considérations relatives aux appareils
--	---	---	--

Contexte

Compte tenu de l'augmentation de popularité de l'option « Apportez vos appareils personnels » et du télétravail, il est important de faire attention à la façon dont les appareils sont utilisés pour mener des activités commerciales. Chaque type d'appareil, qu'il s'agisse d'un routeur, d'un téléphone intelligent, d'un ordinateur portable ou d'une tablette, peut être utilisé pour effectuer un travail à distance. Si l'appareil n'est pas protégé correctement, le travail pourrait être compromis.

Il est important de se rappeler que ces appareils et les logiciels qui peuvent être utilisés sur ceux-ci doivent servir uniquement pour des travaux non classifiés et non sensibles. La présente page contient quelques conseils et astuces, ainsi que certains risques et problèmes de sécurité courants qui sont associés au modèle « Apportez vos appareils personnels ».

Risques et préoccupations en matière de sécurité

Les appareils personnels dans un milieu de travail organisationnel peuvent créer des risques pour la sécurité, notamment :

- Cible pour l'ingénierie sociale – Les attaquants adaptent les attaques à certaines personnes en fonction de la collecte de données ou de renseignements sur les champs d'intérêt personnels.
- Perte et fuites de données – Il s'agit de données de nature délicate complètement effacées ou détruites ou diffusées à des personnes qui ne devraient pas y avoir accès.
- Manque de gestion des mises à jour – Les attaquants peuvent tirer parti d'un logiciel désuet et défectueux pour accéder à un appareil et l'exploiter.
- Perte d'un appareil ou d'une ressource – Il s'agit du vol ou de la perte d'un appareil qui ne peut être comptabilisé(e).
- Faibles antivirus ou pare-feu – Les attaquants peuvent exploiter ces faiblesses en matière de sécurité pour accéder à un appareil.

Il s'agit d'un sous-ensemble d'une longue liste d'occasions d'exploitation si un appareil n'est pas sécurisé adéquatement.

Recommandations liées à la sécurité des appareils

On encourage l'utilisation d'appareils personnels dans un milieu non classifié et non sensible. Cependant, lorsque les employés se servent de ces appareils, ils doivent garder à l'esprit les pratiques exemplaires et les recommandations à suivre. Voici quelques moyens généraux de protéger des appareils personnels :

- Verrouillez l'appareil avec un mot de passe robuste, un NIP ou un identificateur biométrique, le cas échéant.
- Effectuez régulièrement des mises à jour des applications logicielles et des systèmes d'exploitation.
- Ne laissez pas les appareils sans surveillance, surtout dans les endroits publics.
- Évitez d'installer des applications non approuvées.
- Désactivez, ou évitez d'utiliser, la fonction « Se souvenir de moi » pour le stockage des mots de passe et des justificatifs d'identité.
- Évitez d'utiliser des bornes de recharge gratuites.
- Soyez conscient de votre environnement.

Téléphones intelligents et appareils mobiles connexes

Les téléphones intelligents nous permettent de nous connecter directement aux conférences, aux réunions d'équipe et aux applications de collaboration. Si ces appareils ne sont pas protégés, ces appareils peuvent devenir une cible facile pour les attaquants.

Bien qu'il existe de nombreux appareils mobiles comme les téléphones intelligents, les montres intelligentes, les tablettes, les ordinateurs portatifs, etc., les appareils permettent habituellement les mêmes types de communications et sont généralement dotés des mêmes paramètres de sécurité. Dans certains cas, des mêmes systèmes d'exploitation.

Bluetooth

Pour les appareils qui ont des fonctionnalités Bluetooth, suivez les conseils ci-dessous :

- Désactivez la fonction Bluetooth lorsque vous ne l'utilisez pas.
- Désactivez les modes « découverte » ou « diffusion ».
- Évitez de jumeler l'appareil par Bluetooth dans un endroit public.
- N'utilisez pas de clavier Bluetooth pour taper du texte sensible.
- Utilisez seulement des appareils reconnus, comme des écouteurs personnels ou des systèmes audio résidentiels.
- Pour les appareils Apple, désactivez la fonction AirDrop.

Authentification sur les appareils mobiles

Il existe de nombreuses façons de sécuriser des appareils mobiles, notamment les données biométriques, comme les empreintes digitales ou rétir ainsi que les phrases de passe ou les NIP classiques. Même si tous ces moyens valent mieux que l'absence complète d'authentification, il est import les phrases de passe soient robustes, et que les NIP soient aléatoires et difficiles à deviner. Un exemple de ce qu'il NE faut PAS faire est d'utiliser soi de naissance comme NIP. Ce NIP, qui est facile à deviner même par les attaquants les moins futés, peut rendre votre appareil et vos données vuln aux attaques.

Lorsque vous configurez l'authentification de ces appareils, tenez compte des éléments suivants :

- Évitez d'utiliser des numéros, des phrases ou des noms personnels lors de la création d'un mot de passe. Essayez de vous servir de quelque chos les gens ne peuvent peut-être pas deviner. Un exemple facile à retenir serait d'utiliser la première lettre de chaque mot d'une phrase. Par exemple, phrase « J'ai joué au hockey de compétition quand j'étais enfant et mon numéro était 19! » pourrait être convertie en un mot de passe comme « jjahdcqjeemne19! »
- Créez des mots de passe complexes comprenant des caractères spéciaux (« @ », « # », « & », « _ »), des chiffres et des majuscules et des minusc
- Évitez de remplacer des lettres ou des symboles par des chiffres. Par exemple, « MOTDEP@\$\$E1 » n'est pas un mot de passe sécurisé.
- Activez l'authentification à deux facteurs (A2F). Choisissez de vous authentifier au moyen d'une application d'authentification qui fournit un mot de à usage unique. La plupart du temps, le message texte est le deuxième facteur par défaut, mais il peut être remplacé par une méthode appelée « échange de cartes SIM ».
- Évitez d'utiliser la fonction « Se souvenir de moi » pour les applications et les sites Web.

Médias sociaux et messagerie

Les services de médias sociaux espionnent notre appareil. La plupart du temps, ils ont un vaste accès à des zones d'un appareil qui ne sont habitue pas associées à des applications de médias sociaux comme Facebook, Instagram et Twitter. Afin de protéger vos appareils et vos renseignements personnels, songez à prendre les mesures suivantes :

- Utilisez les médias sociaux uniquement sur des appareils personnels.
- Ayez une phrase de passe ou un mot de passe robuste.
- Utilisez l'authentification à deux facteurs, dans la mesure du possible.
- Évitez de publier des détails précis liés au travail, comme l'emplacement du bureau, les travaux en cours, les images des postes de travail et les tâches des employés.
- Restreignez l'accès de l'application de médias sociaux. Pour ce faire, désactivez l'accès à la caméra, au registre des appels téléphoniques, aux messages textes, etc., si possible.
- Faites preuve d'intelligence! Réfléchissez à ce que vous publiez. N'affichez pas quelque chose que vous ne seriez pas à l'aise de crier dans la rue dans un endroit public.

Appareils de réseautage et dispositifs Internet

Services d'informatique en nuage

Les fournisseurs de services d'informatique en nuage offrent des outils de bureau ainsi que des services qui permettent le stockage de fichiers, le l'envoi et la réception de courriel et l'accès à distance (pour n'en nommer que quelques-uns). On peut accéder à ces produits et services en se connectant à un panneau de commande ou à un serveur.

Les pratiques exemplaires en matière d'utilisation de ces services comprennent le chiffrement de données sensibles, l'utilisation de logiciels anti-malware de services de sauvegarde procurés par le fournisseur de services d'informatique en nuage (FSIN), ainsi que la recherche de l'endroit où les données sont stockées physiquement.

Retrieved from https://wiki.gccollab.ca/index.php?title=Considérations_relatives_aux_appareils&oldid=24251

This page was last edited on 28 April 2020, at 10:03.

Content is available underCreative Commons Attribution 4.0 International Licenseunless otherwise noted.