CONSEIL CANADIEN DU COMMERCE DE DÉTAIL

CYBERSÉCURITÉ AU DÉTAIL

MODULE 1

PRINCIPES DE BASE DE LA CYBERSÉCURITÉ POUR LES DÉTAILLANTS

Sécuriser vos appareils, vos biens et votre entreprise.

Un guide pour aider les commerces de détail
à se protéger contre la cybercriminalité

CCCD CONSEIL CANADIEN DU COMMERCE DE DÉTAIL

RCC RETAIL COUNCIL OF CANADA

À propos du Conseil canadien du commerce de détail

Nous sommes le plus grand employeur du secteur privé au Canada, avec plus de 2 millions de Canadiens travaillant dans notre secteur. Le secteur génère annuellement plus de 85 G$ en salaires et avantages sociaux. Les ventes au détail de base (à l'exclusion des véhicules et de l'essence) s'élevaient à plus de 462 G$ en 2022. Nos membres représentent plus des deux tiers des ventes au détail du pays. Nous sommes une association à but non lucratif financée par l'industrie qui regroupe des petites, moyennes et grandes entreprises de vente au détail dans toutes les collectivités du pays. Reconnus comme la Voix des détaillantsMC au Canada, nous représentons fièrement plus de 143 000 vitrines dans tous les formats de commerces de vente au détail, y compris les grands magasins, les épiceries, les magasins spécialisés, les magasins à rabais, les détaillants indépendants, les marchands en ligne et les établissements de restauration rapide.

Le Conseil canadien du commerce de détail remercie pour son appui le Programme de subventions pour des collectivités sûres et dynamiques 2022-2024 du ministère du Solliciteur général.

Ontario

© Conseil canadien du commerce de détail 2023. Tous droits réservés.

Toutes les marques commerciales mentionnées dans le présent document appartiennent à leurs propriétaires respectifs. Il est illégal de copier cette ressource sous quelque forme ou par quelque moyen que ce soit, électronique ou mécanique, y compris la photocopie. En acceptant de recevoir ce document, vous vous engagez à respecter la loi sur les droits d'auteur.

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite ou transmise sous quelque forme ou par quelque moyen que ce soit, ou stockée dans une base de données et un système de recherche, sans l'autorisation écrite préalable du Conseil canadien du commerce de détail. Novembre 2023 – Version 1

Coordonnées du Conseil canadien du commerce de détail :

1881 rue Yonge, bureau 800

Toronto (Ontario) M4S 3C4

Sans frais : 888 373-8245

Courriel : education@retailcouncil.org

Table des matières

i. Introduction 2

ii. Les bases de la cybersécurité 3

iii. Sécuriser le Web 5
- Protection des renseignements personnels et professionnels 5
- Utilisation sûre et sécurisée de l'Internet 6
- Protocole à suivre pour les réseaux sociaux 6
- Protection contre l'attaque par piratage psychologique 7
- Défense contre les maliciels 8
- Pratiques d'authentification appropriées 10

iv. Sécurisation des communications numériques 12

v. Sécurisation des données 15
- Sauvegarde des données 15
- Traitement des renseignements sensibles 16

vi. Sécurisation de l'accès à distance 17
- Les bases de l'informatique à distance 17
- Télétravail 17
- Travail lors de déplacements 17

vii. Sécurisation des appareils numériques 20
- Tablettes et téléphones 20
- Stockage portatif de données 20

viii. Sécurisation de l'espace physique 21

ix. Ressources pour les détaillants 23

i. Introduction

Pour les détaillants d'aujourd'hui, la numérisation du secteur, et du reste du monde qui nous entoure, se traduit par des possibilités illimitées d'entrer en contact avec les clients existants et potentiels, d'étendre leur portée et leurs services, et de maintenir leur pertinence à l'ère de l'innovation et du progrès technologiques. Cependant, le paysage numérique actuel de la vente au détail offre un environnement idéal pour les criminels qui s'attaquent à des victimes sans méfiance en lançant toute une série de cyberattaques.

Les cybercriminels ciblent les sites Web, les adresses électroniques, les comptes sur les réseaux sociaux et toute autre présence numérique d'un détaillant pour s'attaquer à ceux qui semblent les plus vulnérables. De plus, la prévalence et la fréquence de ces attaques n'ont fait qu'augmenter depuis le début de la pandémie de COVID-19. En effet, selon une étude récente de Mastercard, depuis le début de la pandémie, la cybercriminalité a augmenté de 600 % et les cyberattaques de 238 %.

Compte tenu de la prolifération continue de cette tendance néfaste, il est essentiel que tous les types de détaillants, des petits aux plus grands et peu importe où ils se trouvent, prennent les mesures nécessaires pour protéger leurs activités afin de garantir la cybersécurité de leurs appareils, de leurs actifs et de leurs activités.

Pour aider les détaillants à créer un environnement numérique sûr et sécurisé, le Conseil canadien du commerce de détail a élaboré le guide intitulé Principes de base de la cybersécurité pour les détaillants. Il contient beaucoup d'informations utiles, de conseils et de pratiques exemplaires visant à améliorer l'écosystème numérique des détaillants et à les protéger contre la cybercriminalité.

Les conséquences de la cybercriminalité :

- Le coût moyen des atteintes à la sécurité des données au Canada est de 5,64 M$, soit 1 M$ de plus que les moyennes mondiales, et 99 % des victimes reconnaissent que le piratage a nui à leurs activités commerciales*.
- La conséquence la plus fréquente est la perte de données clients, et plus d'un tiers des victimes déclarent que le piratage a mis à mal leurs relations avec les fournisseurs ou les clients*.
- La cybercriminalité et la fraude ont coûté plus de 500 M$ aux Canadiens rien qu'en 2022**.

** Selon l'étude Securing the digital economy de MasterCard.*

*** Selon les données de la GRC.*

ii. Les bases de la cybersécurité

La première étape pour un détaillant qui tente d'améliorer sa cybersécurité est de s'assurer qu'il dispose – en fonction de la taille de son entreprise – d'au moins une personne spécialisée dans la prévention des pertes et la cybersécurité, chargée d'élaborer la stratégie, de l'expliquer au personnel, et d'assurer la maintenance du programme. Cependant, il est aussi important que les autres membres de la direction comprennent au moins les bases de la cybersécurité dans le commerce de détail et le rôle qu'elle joue au sein de l'organisation.

Qu'est-ce que la cybersécurité dans le commerce de détail ?

La cybersécurité dans le commerce de détail fait référence à tous les efforts déployés par un commerce de détail, y compris l'utilisation de technologies soutenant différentes mesures et pratiques, qui sont destinées à contrer les cyberattaques. Autrement dit, la cybersécurité au sein d'un détaillant doit servir à protéger ses systèmes, ses appareils numériques, ses applications, ses renseignements personnels et professionnels sensibles, ses données numériques et ses actifs contre toutes les formes de menaces posées par les cybercriminels, notamment les virus informatiques, et les attaques par rançongiciel.

Quel est l'objectif des efforts déployés par les détaillants en matière de cybersécurité ?

La cybersécurité la plus efficace est souvent ancrée dans trois objectifs non négociables :

Respect de la confidentialité – les détaillants sont en permanence en possession de beaucoup de renseignements importants, y compris des dossiers sur les employés, les clients et les finances. Ces informations doivent rester confidentielles et n'être accessibles qu'aux personnes autorisées.

Maintien de l'intégrité – il est essentiel que tous les actifs et renseignements soient complets, intacts et non corrompus afin de maintenir leur intégrité.

Assurer l'accès – il est extrêmement important de maintenir l'accès à tous les systèmes de l'organisation, y compris les réseaux et les serveurs, les services et les renseignements lorsque l'entreprise ou ses clients en ont besoin.

Comment les détaillants peuvent-ils maintenir un programme de cybersécurité efficace ?

Afin de garantir la mise en place et l'exécution d'un programme et d'une stratégie de cybersécurité efficaces, les détaillants et leurs équipes chargées de la cybersécurité doivent respecter un certain nombre d'exigences permanentes :

Détermination des actifs – les détaillants devront identifier les actifs qu'ils souhaitent protéger dans le cadre de leur programme de cybersécurité, ce qui inclut généralement les actifs détenus ou gérés par l'entreprise.

Définition des menaces – il est essentiel de définir toutes les menaces ainsi que leurs éventuelles répercussions sur les actifs.

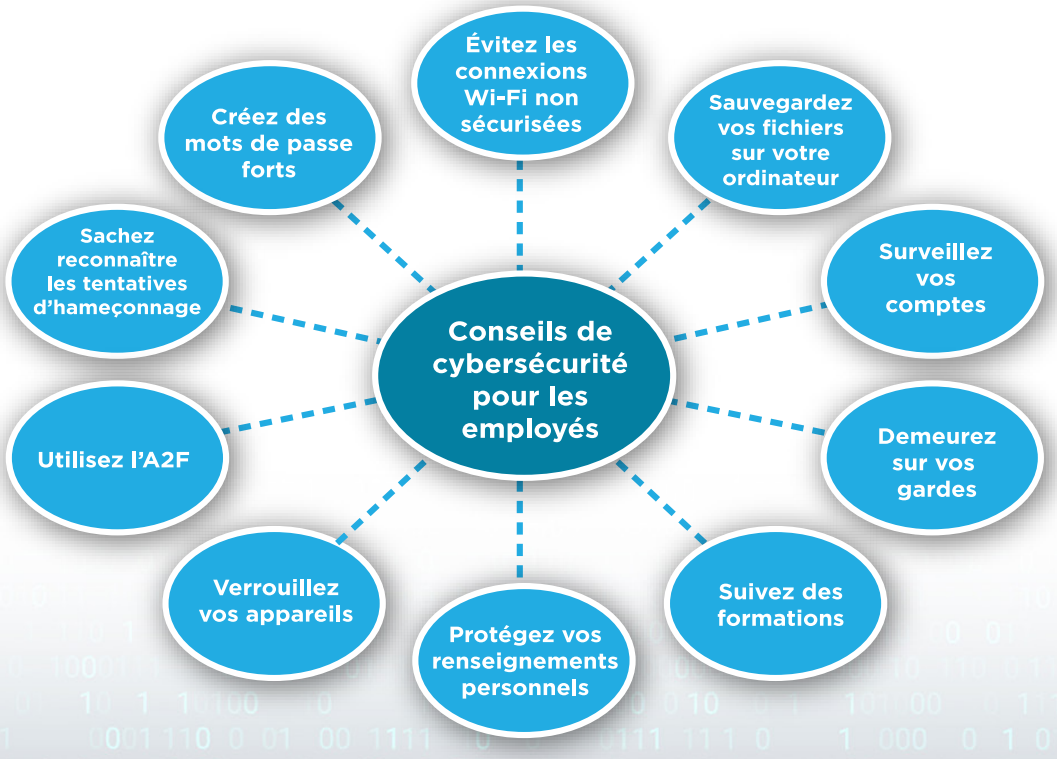
Mise en place de mesures de sauvegarde – après avoir déterminé les actifs et défini les menaces, des mesures de sauvegarde doivent être mises en place à des fins de prévention et d'atténuation.

Contrôle continu – les détaillants peuvent gérer et évaluer correctement l'efficacité de leurs programmes de cybersécurité grâce à un contrôle constant et continu des mesures de protection mises en place.

Réaction rapide – il est essentiel pour les détaillants et leurs équipes de cybersécurité de réagir rapidement aux problèmes de cybersécurité lorsqu'ils se produisent, en temps réel, afin de maintenir l'efficacité de leurs programmes.

Adaptation et mise à jour – il est tout aussi essentiel pour les détaillants d'adapter et de mettre à jour en permanence leurs systèmes et leurs mesures de protection, car les menaces évoluent constamment.

Conseils aux employés en matière de cybersécurité :



iii. Sécuriser le Web

Lorsqu'il s'agit de sécuriser l'écosystème numérique de la vente au détail, il est logique de commencer par protéger tout ce qui touche l'Internet. Compte tenu de la quantité d'activités sur le Web menées par les détaillants et leur personnel, qui peuvent inclure la saisie d'informations personnelles et professionnelles en ligne, la navigation sur Internet et les interactions avec les réseaux sociaux, en plus de la possibilité d'attaques par piratage psychologique ou par maliciels, une approche holistique de la protection des actifs doit être adoptée.

Protéger les informations personnelles et professionnelles en ligne

Il existe un certain nombre de situations différentes au sein d'un détaillant qui peuvent nécessiter qu'un employé saisisse des informations personnelles et/ou professionnelles en ligne, qu'il s'agisse de travailler avec des clients et des partenaires, de remplir des formulaires d'abonnement à des bulletins d'information et à des magazines ou des formulaires de commande de fournitures de bureau. Il peut s'agir de détails à la fois privés et confidentiels révélant les noms complets, les numéros d'assurance sociale, les adresses électroniques, les numéros de téléphone, les adresses physiques, les informations bancaires, ainsi que des détails liés à un certain nombre d'autres actifs et entités. Chaque fois que ce type d'information est saisi, il existe des cybermenaces distinctes et des risques connexes.

Afin de protéger correctement et efficacement toute organisation de vente au détail contre les cybercriminels, il est impératif que ses employés, de la direction au personnel de première ligne, comprennent l'importance de la sécurité Web et la signification qu'elle représente pour toutes les personnes concernées. Les cybercriminels s'attaquent aux personnes vulnérables et élaborent leurs attaques sur la base d'informations personnelles et professionnelles qu'ils ont recueillies en accédant illégalement à des systèmes informatiques. Cela dit, leur incidence peut être réduite considérablement si tous les employés de l'organisation adhèrent à quelques pratiques exemplaires simples :

Légitimité et confiance – veillez à ce que tous les employés qui utilisent les appareils informatiques de l'organisation comprennent l'importance de ne visiter que des sites Web légitimes et de confiance, y compris s'il s'agit d'y saisir des renseignements.

Vérification du destinataire – avant de communiquer des informations personnelles ou professionnelles à qui que ce soit, les employés doivent d'abord vérifier la fiabilité du destinataire.

Questions – chaque fois que quelqu'un demande des informations personnelles ou professionnelles, les employés doivent demander les raisons pour lesquelles ces informations sont nécessaires. Si la réponse fournie ne suffit pas, les employés doivent être en mesure de refuser de fournir les informations demandées.

Maintien des mesures de protection – malgré les raisons qui peuvent être invoquées, aucune ne peut justifier la suppression ou la désactivation des mesures de sécurité ou des mesures de protection, telles que les logiciels antivirus et de protection contre les maliciels, qui ont été mises en place sur les ordinateurs et les réseaux par l'organisation.

Garantir des pratiques Internet sûres et sécurisées

Les détaillants et leurs employés dépendent énormément de l'Internet pour accomplir leurs tâches quotidiennes. Qu'il s'agisse de courriels de tous les jours, de recherches ou d'activités d'achat courantes, il existe plusieurs raisons pour lesquelles une organisation de vente au détail et ses employés doivent naviguer sur l'Internet. Bien que l'utilisation d'Internet soit aujourd'hui inhérente et répandue, et qu'elle fasse partie des activités quotidiennes de presque tous les détaillants, il est toutefois souhaitable que ces derniers s'assurent que tous les membres de leur organisation prennent les précautions nécessaires lorsqu'ils naviguent sur le Web.

Politiques et protocoles – c'est une très bonne idée pour les entreprises de vente au détail de préciser ce qu'elles attendent de leurs employés en ce qui concerne les activités et le comportement de navigation sur Internet. Pour ce faire, les détaillants doivent élaborer leur propre politique d'utilisation de l'Internet, à l'interne, qui explique clairement aux employés ce qu'il faut faire et ne pas faire en matière de connexion à l'Internet à partir des systèmes et des appareils de l'entreprise.

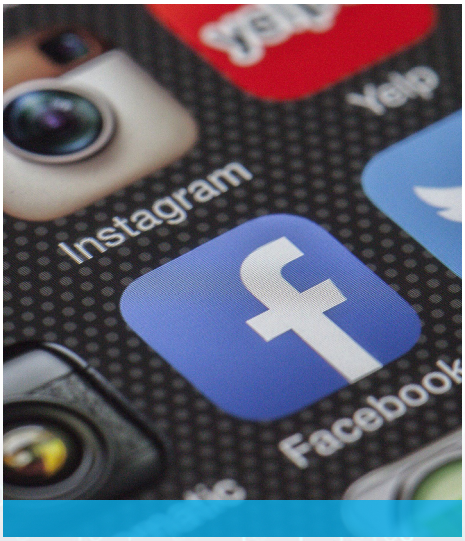
Formation des employés – après avoir élaboré des politiques encadrant l'Internet à l'intention des employés, il est impératif de leur fournir une formation complète sur la politique d'utilisation d'Internet.

Promouvoir la sensibilisation – en plus de la formation que les employés reçoivent de la part des détaillants sur leur politique d'utilisation d'Internet, il doit aussi y avoir la promotion continue de cette politique pour s'assurer que tout le monde la comprenne.

Mettre en place des outils d'évaluation des sites – comme précaution supplémentaire, les entreprises de vente au détail peuvent facilement équiper leurs navigateurs Internet d'un outil d'identification de l'extension des sites pour les évaluer.

Assurer la sécurité des recherches – dans le cadre de leur formation continue, les employés doivent apprendre à confirmer que les URL des sites qu'ils visitent sont sûres et sécurisées en utilisant un outil d'identification.

Établir des protocoles pour les réseaux sociaux



Parmi tous les canaux qui ont vu le jour au cours des dernières années, les sites Web de réseaux sociaux tels que Facebook, X, Instagram, Pinterest et autres sont sans doute les plus influents, offrant aux détaillants beaucoup de possibilités d'engagement des clients et de marketing pour renforcer leurs relations et leur marque. Cependant, étant donné la popularité de ces sites, ils deviennent de plus en plus des cibles pour les cybercriminels qui cherchent à tirer profit des vulnérabilités en ligne afin de voler des informations personnelles et professionnelles.

Face à cette menace, il est extrêmement important que les entreprises de vente au détail intègrent le protocole et les pratiques exemplaires en matière de réseaux sociaux dans leur politique d'utilisation d'Internet, en indiquant aux employés le comportement à adopter sur ces sites.

Désigner des personnes chargées des réseaux sociaux – il est conseillé de désigner un petit nombre de personnes qui seront responsables de l'activité de l'organisation dans les réseaux sociaux. L'activité doit être limitée à ces personnes autorisées.

Définir les renseignements pouvant être divulgués – les détaillants doivent définir clairement le type d'informations qui peuvent être saisies sur les réseaux sociaux. Cela peut être inclus dans la politique d'utilisation de l'Internet.

Ne pas inclure d'informations sensibles – les employés ne doivent jamais inclure d'informations personnelles ou professionnelles sensibles dans les publications de l'organisation sur les réseaux sociaux.

Se méfier des applications de réseautage – il est judicieux que les entreprises de vente au détail et leurs employés évitent d'utiliser les applications de réseautage, qui sont souvent créées et gérées par des tiers et donc pas forcément aussi sécuritaires que les sites Web correspondants.

Communiquer avec prudence – lorsqu'ils communiquent avec quelqu'un sur des sites de réseaux sociaux, les employés du commerce de détail doivent faire preuve de prudence, en particulier lorsqu'on leur demande des renseignements sur l'entreprise ou l'un des employés.

Réviser les renseignements avant de les publier – c'est toujours une bonne idée d'être minutieux lorsque l'on communique sur des réseaux sociaux. Cela signifie qu'il faut revoir l'information avant sa publication.

De nombreuses entreprises de vente au détail ont également pour politique d'autoriser leurs employés à consulter leurs comptes de réseaux sociaux personnels lorsqu'ils sont au travail..

Protection contre les attaques par piratage psychologique

Les moyens de perpétrer des cyberattaques se multiplient, tout comme les manipulations avec lesquelles elles sont déployées. En effet, l'attaque par piratage psychologique est l'une des tactiques de manipulation les plus efficaces dont disposent les cybercriminels pour obtenir des renseignements. En trompant les employés, les cybercriminels peuvent accéder aux systèmes informatiques, et donc évidemment aux renseignements.

En s'appuyant sur le peu d'informations dont ils disposent déjà, ils communiquent avec les employés, que ce soit en ligne, par courriel ou par téléphone, et tentent de gagner leur confiance. Souvent, ils prétendent être des clients ou des partenaires de l'entreprise ou des proches d'un collègue. Ils peuvent même présenter de fausses « preuves » de leur lien « légitime » avec l'entreprise. Certains vont jusqu'à se faire passer pour un fonctionnaire ou une autre figure d'autorité, en demandant des informations

telles que des numéros de téléphone ou des données de compte. Dans certains cas, ils peuvent demander aux individus d'ouvrir des courriels et des pièces jointes ou de visiter certains sites Web.

Puisqu'il s'agit de manipulation, la plupart des victimes ne se doutent de rien avant qu'il ne soit trop tard. Ce n'est qu'après qu'ils se rendent compte des conséquences très réelles de ce type d'attaque. Afin d'éviter ces situations et de protéger correctement ses actifs et son personnel, les détaillants doivent s'assurer que leurs employés sont conscients de ces escroqueries et qu'ils demeurent vigilants.

Être aux aguets – il est conseillé d'informer tous les employés qu'ils doivent se méfier de tous les courriels, appels téléphoniques et visites qu'ils reçoivent de personnes prétendant être liées d'une manière ou d'une autre à l'entreprise ou à une personne travaillant au sein de celle-ci.

Vérifier – valider l'identité de toute personne demandant un type d'information en demandant un document officiel.

Suivre les pratiques exemplaires en matière de sécurité sur le Web – en cas de doute sur le protocole à suivre, il convient de conseiller aux employés de se référer à toutes les autres pratiques exemplaires concernant la conduite à tenir en matière de courriel, de réseaux sociaux, d'activités sur Internet et d'autres activités sur le Web.

Se défendre contre les maliciels (logiciels malveillants)

Étant donné que l'ensemble du paysage numérique et de l'écosystème de la vente au détail repose sur une série infinie de logiciels, de systèmes, de programmes et d'applications auxquels il est connecté, les menaces posées par les maliciels sont innombrables et, le plus souvent, très perturbatrices et destructrices.

Qu'est-ce qu'un maliciel ?

Les maliciels, ou logiciels malveillants, sont des logiciels conçus, développés et déployés dans le but d'endommager un système et/ou d'obtenir illégalement des informations. Ces logiciels sont conçus pour ne pas être détectés. C'est pourquoi ils sont souvent capables de s'infiltrer dans les ordinateurs de bureau, les ordinateurs portables, les téléphones et les tablettes sans être détectés ou supprimés par les dispositifs de sécurité.

Quels sont les types de maliciels existants ?

Il existe plusieurs types de maliciels. Le plus courant, et sans doute le plus efficace, est le « virus », qui est capable d'infecter les systèmes d'exploitation pour ensuite faire une copie de lui-même et d'infiltrer d'autres appareils. Cependant, il existe d'autres types de maliciels dont les commerces de détail et leurs employés doivent être conscients. Voici quelques exemples :

Vers – semblables aux virus, les vers se propagent de manière indépendante, sans avoir besoin de s'attacher à d'autres fichiers ou programmes.

Chevaux de Troie – déguisés en logiciels légitimes, les chevaux de Troie incitent les utilisateurs à les installer.

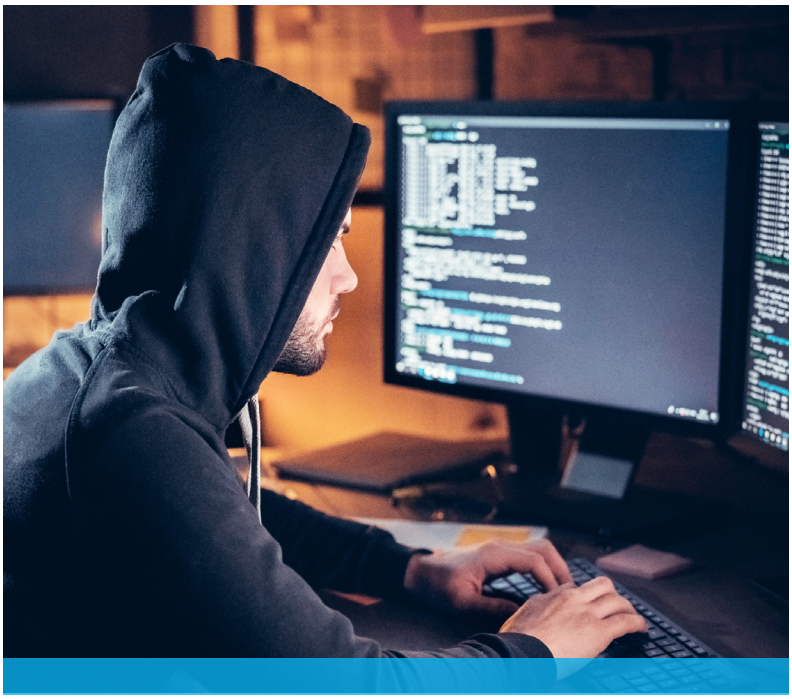
Rançongiciels – le cryptage des fichiers sur l'ordinateur d'une victime permet aux attaquants de demander une rançon afin d'en rétablir l'accès.

Logiciels espions – conçus pour recueillir secrètement des informations sur les activités d'un utilisateur, généralement à son insu ou sans son consentement, les logiciels espions peuvent enregistrer les frappes au clavier, surveiller les habitudes de navigation et collecter des informations personnelles auprès des personnes qui ne se doutent de rien.

Logiciels de publicité – affichage de publicités indésirables sur l'appareil d'un utilisateur. Il n'est pas toujours malveillant, mais le logiciel de publicité peut être intrusif et nuire à la performance du système.

Quel est l'objectif des maliciels ?

Les maliciels se présentent le plus souvent sous la forme de pièces jointes à des courriels ou de téléchargements sur des sites Web. Ils sont conçus pour s'infiltrer dans les systèmes d'exploitation, infecter les fichiers, les corrompre ou les supprimer complètement, ce qui permet la capture illégale d'informations sensibles.



Que peuvent faire les détaillants ?

Les maliciels sont souvent incroyablement efficaces, mais les entreprises de vente au détail peuvent prendre certaines mesures pour protéger leurs systèmes commerciaux et leurs informations numériques.

Logiciel anti-maliciel – en raison de la prolifération de différents types de maliciels, il existe aujourd'hui une gamme de logiciels anti-maliciel qui permettent aux utilisateurs d'analyser tous les fichiers entrant dans l'organisation et de bloquer tout ce qu'ils jugent suspect ou qui contient des maliciels.

Pare-feu – les détaillants peuvent aussi vouloir installer des pare-feu informatiques afin d'empêcher la connexion à des sites Web malveillants et néfastes. De plus, de nombreux pare-feu sont capables d'empêcher de nombreux types de maliciels de pénétrer dans le système.

Formation des employés – parallèlement à la mise en place de logiciels anti-maliciel et de pare-feu, tous les employés de l'entreprise doivent recevoir une formation et de l'éducation continue sur la sécurité.

Tenir compte des avertissements – tous les employés de l'entreprise doivent être conscients des avertissements figurant sur les sites Web et dans les courriels concernant des contenus potentiellement malveillants, et en tenir compte.

Signaler les alertes – si un employé reçoit un rapport ou un avertissement provenant d'un logiciel anti-maliciel de l'organisation, il doit le signaler immédiatement à un supérieur.

Isoler les courriels et les fichiers suspects – il faut conseiller aux employés de ne jamais ouvrir ou envoyer à une autre personne des courriels ou des pièces jointes suspects.

Garantir des pratiques d'authentification appropriées

Lorsque l'on traite des quantités importantes de données et d'informations sensibles, il est extrêmement important que les pratiques d'authentification conçues par les détaillants soient suivies par tous les employés.

Mots de passe

Couramment utilisés pour protéger différents comptes et systèmes contenant une pléthore d'informations et d'outils professionnels, les mots de passe constituent une couche de protection nécessaire dans l'écosystème numérique de la vente au détail. Cependant, s'ils ne sont pas utilisés correctement, les mots de passe peuvent devenir une vulnérabilité au sein des entreprises et les exposer davantage aux menaces des cybercriminels.

Maintenir le contrôle et la confidentialité – veillez à ce que les employés comprennent l'importance de garder leurs mots de passe en sécurité et inconnus de leur entourage.

Éviter d'utiliser des mots de passe faibles – les employés doivent éviter d'utiliser des mots de passe faciles à deviner qui peuvent permettre à d'autres personnes d'accéder à leurs fichiers et à leurs informations.

Éviter d'utiliser le même mot de passe – il convient de préciser à tous les employés qu'ils doivent non seulement éviter d'utiliser des mots de passe faciles à deviner, mais aussi éviter d'utiliser le même mot de passe pour chaque compte et chaque appareil.

Modifier fréquemment le mot de passe – les mots de passe doivent être modifiés fréquemment par tous les employés afin d'éviter la complaisance et de réduire la prévisibilité.

Établir une politique – il peut être judicieux pour certains détaillants d'élaborer une politique en matière de mots de passe qui établit des règles simples à suivre lors de la création d'un mot de passe.

Éviter les expressions courantes et simples – lors de la création de mots de passe, les employés doivent éviter d'utiliser des expressions courantes telles que « mot de passe » ou « entrer », des séquences de chiffres simples telles que « 1234 », et des noms personnels faciles à deviner tels que le prénom d'un enfant.

L'importance de la longueur – plus le mot de passe comporte de caractères, plus il est efficace. Veillez donc à créer des mots de passe d'au moins huit caractères.

Force combinée – les mots de passe sont également plus forts lorsque plusieurs types de caractères (lettres majuscules, lettres minuscules, chiffres et caractères spéciaux) sont utilisés.

Phrases de passe

Pour les détaillants qui veulent une forme de sécurité plus poussée, l'utilisation de phrases de passe au lieu de mots de passe pourrait être une solution judicieuse.

Par exemple, au lieu d'utiliser le mot de passe « G0bLUe ! », une phrase de passe telle que « Ceuxqui-resterontserontchampions! » devient beaucoup plus difficile à deviner. De plus, des sigles peuvent être utilisés à la place de longues phrases (par exemple, « bravoauxchampionsquiileresterontpourtoujours! » devient « brvxchmpnsqlrstrntprtjrs! »), ce qui nécessite moins de caractères à taper, mais maintient l'efficacité de la protection et de la sécurité.

Les cybercriminels créent constamment des logiciels conçus pour pirater et deviner les mots de passe. Dans ce contexte, certains détaillants pourraient envisager d'utiliser l'un des nombreux outils en ligne gratuits qui démontrent aux utilisateurs la force ou la faiblesse relative d'un mot de passe ou d'une phrase de passe.

Authentification à deux facteurs

Bien plus difficiles à deviner que les mots de passe ou les phrases de passe, les authentifications à deux facteurs permettent d'ajouter une couche de complexité et de sécurité aux systèmes des détaillants.

Essentiellement, comme son nom l'indique, l'authentification à deux facteurs exige que la personne ou le système demandant une autorisation fournisse deux éléments d'authentification – un facteur connu par la personne ou le système (comme un mot de passe), et le second facteur est un élément, permanent ou temporaire, qui peut être utilisé pour valider l'identité de la personne ou du système (comme une empreinte digitale ou un mot de passe temporaire).

Alors que les technologies continuent de devenir plus puissantes et intuitives, et que les capacités de l'intelligence artificielle et de l'apprentissage automatique augmentent sans cesse, l'authentification à deux facteurs devient de plus en plus nécessaire pour renforcer la protection et la sécurité des actifs, des informations et des systèmes d'un détaillant.

Signalement des attaques

Si un employé est victime d'un acte de cybercriminalité, il ne doit pas hésiter à le signaler à ses supérieurs. Si l'on soupçonne que l'attaque a compromis l'entreprise d'une manière ou d'une autre, le détaillant doit :

Signaler l'incident aux forces de l'ordre

Signaler l'incident au système de signalement des incidents de cybercriminalité et de fraude ici, ce qui informe la Gendarmerie royale du Canada (GRC), le Centre national de coordination en cybercriminalité (CNC3) et le Centre antifraude du Canada (CAFC), afin de protéger l'organisation aujourd'hui et de l'aider à se prémunir contre des menaces similaires à l'avenir.

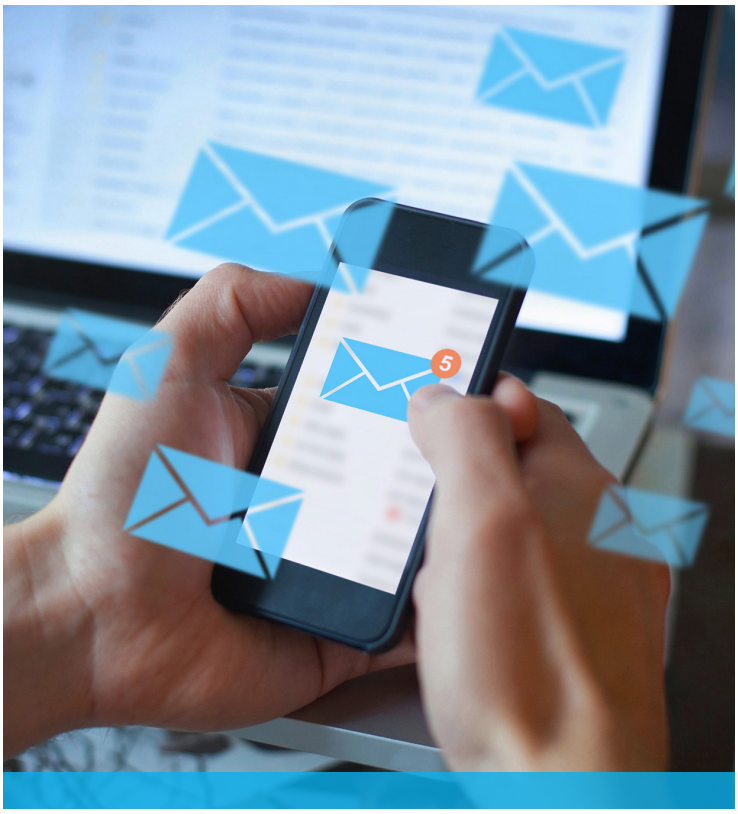
iv. Sécurisation des communications numériques

La plupart, sinon la totalité, des communications entre collègues, associés et partenaires commerciaux se font aujourd'hui par courriel. Toutefois, comme nous l'avons mentionné, les cybercriminels ciblent de plus en plus le courriel pour infiltrer les systèmes des détaillants afin de s'emparer d'informations personnelles et professionnelles sensibles.

Afin de garantir une protection et une sécurité optimales lors de l'utilisation du courriel, tous les employés doivent connaître les moyens les plus courants par lesquels les cybercriminels tentent d'utiliser le courriel.

Pourriel

Représentant la grande majorité des communications électroniques envoyées sur l'Internet, le pourriel est un courriel non sollicité et envoyé sans l'autorisation du destinataire. Il est souvent déguisé en promotion de produit ou de service ou en offre à laquelle il est possible de répondre en cliquant sur un lien ou en visitant un site Web. Par procuration, le pourriel est incroyablement intrusif et ennuyeux à recevoir. Cependant, si l'on clique sur des liens ou si l'on ouvre des pièces jointes, des maliciels sont souvent téléchargés sur l'appareil utilisé, ce qui ralentit les réseaux et les serveurs et entraîne une augmentation des coûts et une baisse de la productivité.



Les entreprises de vente au détail devront veiller à ce que leurs employés soient attentifs aux messages et aux courriels qu'ils reçoivent et à ce qu'ils fassent preuve de prudence pour décerner les pourriels.

Expéditeur inconnu – les employés doivent traiter avec prudence toute communication provenant d'un expéditeur inconnu.

Fautes d'orthographe – afin de contourner les filtres anti-pourriel et d'autres dispositifs de sécurité, les cybercriminels commettent intentionnellement des fautes d'orthographe dans la ligne d'objet du courriel. Les employés ne doivent pas ignorer ce signe que quelque chose cloche.

Formulation maladroite – au même sens que les fautes d'orthographe, le texte peut avoir une formulation maladroite ou inhabituelle, indiquant que l'expéditeur n'est peut-être pas légitime.

Méfiance – si le message promet des offres qui semblent trop belles pour être vraies, s'il demande de cliquer sur des liens ou s'il demande des informations personnelles ou professionnelles, il s'agit probablement d'un pourriel.

Hameçonnage

Étant une sorte de pourriel extrêmement pointu et spécialisé, les courriels d'hameçonnage sont conçus pour ressembler exactement à un message légitime et sont souvent déguisés en communications émanant d'un organisme officiel, par exemple, une agence gouvernementale ou une institution bancaire. Souvent, ces types de pourriels sont élaborés avec soin, parfois en utilisant de véritables logos, polices de caractères, palettes de couleurs et images, et sont impossibles à distinguer d'une communication réelle.

L'objectif des courriels d'hameçonnage est similaire à celui du pourriel, mais leurs tactiques sont un peu différentes. Plutôt que de promouvoir un service ou un produit, les courriels d'hameçonnage utilisent généralement un ton utile pour susciter la confiance ou un message intimidant pour susciter la peur, dans le but d'obtenir une réponse ou de cliquer sur un lien.

Le champ d'application des attaques par hameçonnage s'élargit constamment, mais les attaquants les plus fréquents ont tendance à utiliser l'une de ces quatre tactiques :

Intégrer dans les courriels des liens qui redirigent les utilisateurs vers un site Web non sécurisé demandant des informations sensibles.
Installer des chevaux de Troie par le biais d'une pièce jointe malveillante ou de publicités sur un site Web qui permettent aux intrus d'exploiter des failles et d'obtenir des informations sensibles.
Usurper l'adresse de l'expéditeur d'un courriel pour faire croire qu'il s'agit d'une source fiable et demander des informations sensibles.
Tenter d'obtenir des informations sur l'entreprise par téléphone en se faisant passer pour un fournisseur ou un service informatique connu de l'entreprise.

Moyens de bloquer les attaques d'hameçonnage :

Les employés doivent toujours se méfier des attaques par hameçonnage, en particulier lorsqu'ils ne connaissent pas l'expéditeur. Voici cinq pratiques exemplaires à suivre pour éviter que les employés ne deviennent des victimes :

1. **Ne pas divulguer d'informations personnelles ou financières dans un courriel –** assurez-vous que les employés savent qu'ils ne doivent pas répondre à des sollicitations par courriel pour obtenir ces informations, y compris en cliquant sur les liens envoyés dans les courriels.
2. **Vérifier la sécurité des sites Web –** il s'agit d'une précaution essentielle à prendre avant d'envoyer des informations sensibles sur l'Internet. <http> indique que le site Web n'a appliqué aucune mesure de sécurité, tandis que <https> indique qu'il l'a fait. Dans cette optique, les employés doivent adopter des habitudes de navigation sûres tout en comprenant que les sites Web qui ne servent pas un objectif professionnel légitime sont également plus susceptibles de contenir des liens nuisibles.

3. **Faire attention aux URL des sites Web –** tous les courriels ou liens de courriels ne ressemblent pas à des attaques d'hameçonnage, de sorte que les employés peuvent parfois être induits en erreur et avoir un faux sentiment de sécurité. De nombreux sites Web malveillants trompent les utilisateurs en imitant des sites Web légitimes. L'un des moyens de déterminer si le site Web est légitime ou non est de regarder l'URL (si elle n'est pas cachée derrière un texte non descriptif). Les employés peuvent également être en mesure de détecter et de contourner le système en trouvant des variations dans l'orthographe ou un domaine différent (.com par rapport à .net).
4. **Vérifier les demandes de courriel suspectes –** communiquer directement avec l'entreprise dont les courriels semblent provenir. Si un employé reçoit un courriel qui semble suspect de la part d'une entreprise connue, telle qu'une banque, prenez contact avec la banque en utilisant d'autres moyens que la réponse à l'adresse électronique suspecte. Il est préférable de contacter l'entreprise en utilisant les informations figurant sur un relevé de compte – et NON les informations fournies dans le courriel.
5. **Garder le tout bien en ordre –** l'utilisation du système d'exploitation, des logiciels et du navigateur Web les plus récents, ainsi que d'un antivirus et d'une protection contre les maliciels, constitue la meilleure défense contre les virus, les maliciels et les autres menaces en ligne. Demandez à votre direction et à votre service informatique de vous indiquer les navigateurs Web approuvés et sûrs.

Que faire des courriels d'hameçonnage ?

Il est important d'informer les employés sur la prévalence des escroqueries par hameçonnage et au protocole concernant la manière de signaler une communication suspecte. Dans la plupart des cas, les employés doivent être informés qu'ils doivent éviter d'envoyer et de partager le message avec d'autres personnes, et qu'ils doivent plutôt le sauvegarder pour le montrer à un supérieur. Ne supprimez pas ce type de messages suspects, même si un supérieur en a été informé.

De plus, contactez le responsable de la sécurité informatique de votre organisation et informez-le de ce courriel. La sécurité informatique voudra une copie du courriel afin d'enquêter et de bloquer la source. Elle vous fournira des instructions à suivre.

v. Sécurisation des données

Avec l'évolution de la numérisation, les détaillants sont en possession d'une énorme quantité de données qu'ils traitent en permanence. Compte tenu de l'importance des données qu'ils collectent chaque jour pour la croissance de leurs entreprises et l'optimisation de leurs opérations, il est logique qu'elles soient sécurisées et protégées aussi rigoureusement que n'importe quel autre actif.

Pourquoi sauvegarder les données ?

La sauvegarde des fichiers numériques et physiques est une pratique qui permet de conserver les données importantes et de restaurer les fichiers perdus ou endommagés. De plus, et c'est peut-être le plus important, s'ils sont exécutés correctement et à intervalles réguliers, les plans de sauvegarde permettent aux détaillants de se rétablir rapidement en cas de panne du système, de corruption des données ou d'autres problèmes.

Sauvegarde des données

Le moyen le plus efficace pour les détaillants de garantir la bonne conservation des données est d'élaborer un plan de sauvegarde – un plan auquel tous les employés de l'entreprise se conformeront, en adhérant à un ensemble strict de pratiques de sauvegarde.

Sauvegarde fréquente – les employés doivent sauvegarder régulièrement les données conformément au plan de sauvegarde, que ce soit toutes les heures ou tous les jours.

Stockage physique – parallèlement à la fréquence, veillez à ce que les données soient sauvegardées de différentes manières, notamment sur des disques durs physiques, afin d'ajouter une couche de sécurité.

Destruction des données – les données qui n'ont pas été sauvegardées et qui seront éliminées par l'entreprise doivent être détruites adéquatement. Supprimez tous les fichiers numériques et déchiquetez tous les documents physiques afin d'éviter qu'ils ne soient utilisés contre l'entreprise.

Options de sauvegarde

Les entreprises de vente au détail peuvent sauvegarder leurs données de plusieurs manières, afin de garantir leur sécurité à court et à long terme.

Disque dur USB – selon la taille de l'entreprise, les disques durs USB portables ou de bureau peuvent constituer une option de sauvegarde appropriée.

Serveur – idéalement, les données doivent être stockées sur le réseau local (LAN) de l'entreprise et sauvegardées automatiquement à partir de là.

En ligne – les détaillants peuvent également choisir de sauvegarder leurs données sur Internet, ce qui permet à des fournisseurs de services tiers de se charger de la sauvegarde et de la restauration.

Traitement des informations sensibles

Compte tenu de la quantité de données avec lesquelles les détaillants travaillent régulièrement, au moins une partie d'entre elles peut être considérée comme sensible, y compris les informations personnelles des employés, ainsi que les données relatives aux clients et aux finances. En tant que telles, les mauvaises manipulations de ces données peuvent entraîner un accès non autorisé à celles-ci, leur perte, leur manipulation et leur modification, ainsi qu'une série de préjudices pour les entreprises et leurs clients.

Restreindre l'accès – lorsque les données ne sont pas utilisées, qu'il s'agisse de fichiers numériques ou physiques, elles doivent être mises sous clé, avec un accès limité à un petit nombre d'employés, et sécurisées par une combinaison de mesures de protection électroniques et physiques.

Étiqueter correctement – afin de garantir la bonne conservation des données sensibles, les dossiers et les documents doivent être correctement étiquetés et stockés en conséquence.

vi. Sécuriser l'accès à distance

Beaucoup de choses ont changé dans l'environnement des entreprises nord-américaines au cours des dernières années, avec la popularité croissante du travail à distance et l'adoption de ces nouvelles modalités de travail par les entreprises partout dans le monde. Il s'est avéré être un véritable atout pour les entreprises, leur permettant d'économiser du temps et de l'argent, tout en stimulant la productivité des employés. Toutefois, cette évolution des conditions et de l'environnement de travail s'accompagne d'une hausse des risques d'exposition aux cybercriminels et à leurs stratagèmes numériques. En mettant en place les bons contrôles et en garantissant les pratiques exemplaires, il est possible d'atténuer une grande partie de la menace posée par les cybercriminels.

Les bases de l'informatique à distance

Pour les commerces de détail qui ont décidé d'accorder à leurs employés les avantages du télétravail, l'accès à leurs réseaux se fera probablement par Internet. Il s'agit d'un moyen facile et efficace de connecter les employés à leur travail, quel que soit l'endroit où ils se trouvent, mais la connexion par Internet n'est pas considérée comme un moyen sûr d'échanger des informations, car elle offre aux cybercriminels plus de possibilités que jamais d'exploiter les faiblesses des politiques et des pratiques numériques.

C'est pourquoi il est judicieux que les entreprises de vente au détail utilisent un réseau privé virtuel (VPN) sécurisé pour la connexion à leurs réseaux, car un VPN permet de crypter la connexion, ce qui rend la communication et le transfert d'informations inutilisables pour toute personne autre que celle à qui le message a été envoyé.

La plupart conseillent de combiner l'utilisation d'un VPN avec d'autres mesures de protection mentionnées dans ce guide, et de faire en sorte que les employés suivent un ensemble de pratiques exemplaires pour garantir la sécurité de l'accès à distance.

Limiter l'accès à distance aux employés autorisés ayant un besoin professionnel clair. L'accès ne doit s'étendre qu'aux applications, informations et services nécessaires à l'exécution du travail.

Accord d'accès à distance – tous les employés qui bénéficient d'un accès à distance doivent signer un accord d'accès à distance qui décrit et souligne les règles, les responsabilités et les pratiques exemplaires en la matière.

Ajustement de l'accès – il est important de permettre l'ajustement des privilèges d'accès à distance en cas de modification des responsabilités des personnes au sein de l'entreprise.

Attribution d'ordinateurs – c'est une très bonne idée de fournir aux employés un accès à distance avec des ordinateurs professionnels qui ont été configurés et activés avec les logiciels et les mesures de protection décidées par l'entreprise pour améliorer la sécurité et le contrôle.

Étiqueter et enregistrer les informations relatives aux appareils – avant d'attribuer des ordinateurs professionnels et d'autres appareils aux employés ayant un accès à distance, il convient de les étiqueter et d'enregistrer leur numéro de série, afin de faciliter le suivi de leur configuration ou leur récupération en cas de perte ou de vol.

Télétravail

Le mode d'accès à distance le plus courant est le télétravail. C'est un moyen simple et pratique pour les employés de communiquer avec leur employeur. Toutefois, si l'on utilise un ordinateur personnel, on s'expose à des risques supplémentaires. Les entreprises de vente au détail et leurs employés doivent donc se conformer à quelques exigences afin de renforcer la sécurité du travail à domicile.

Restrictions de l'accès sans fil – tous les employés, lorsqu'ils travaillent à domicile sur un ordinateur personnel, doivent connecter leur ordinateur directement à un routeur à l'aide d'un câble Ethernet, et connecter le câble Ethernet au modem, afin d'empêcher toute personne extérieure au réseau d'écouter ou d'intercepter les communications.

Sécuriser le Wi-Fi – il faut conseiller aux employés de sécuriser leur connexion Wi-Fi afin d'empêcher les cybercriminels d'accéder à des informations professionnelles sensibles.

Modifier le nom du réseau par défaut – les employés travaillant à domicile doivent modifier le nom du réseau Wi-Fi par défaut et le mot de passe d'accès au routeur du réseau pour améliorer la sécurité de la connexion.

Chiffrement du réseau – le chiffrement du réseau doit être activé.

Accès limité – en plus des mesures de protection et les dispositifs de sécurité numériques, les employés qui travaillent à domicile sur leur ordinateur personnel doivent veiller à prendre des précautions physiques, en limitant l'accès à l'ordinateur.

Travail lors de déplacements

La numérisation du monde qui nous entoure, associée à une nouvelle réalité professionnelle, signifie que le commerce de détail d'aujourd'hui est en grande partie un commerce portable, qui permet aux employés de travailler où et quand ils le souhaitent, y compris lors de déplacements. Par conséquent, les données et les informations hébergées dans l'écosystème numérique d'un détaillant sont d'autant plus exposées aux risques, ce qui oblige les employés à faire preuve de prudence et à suivre les pratiques exemplaires lorsqu'ils travaillent pendant leurs déplacements.

Éviter les connexions douteuses – lorsqu'ils sont en déplacement, qu'ils travaillent depuis un hôtel ou un aéroport, ou n'importe où ailleurs, les employés doivent toujours éviter d'utiliser des connexions Wi-Fi inconnues ou douteuses. Bien qu'ils soient gratuits, ils ne sont souvent pas très sûrs.

Gardez vos appareils à portée de main – les employés ne doivent jamais, au grand jamais, laisser leurs appareils de travail, qu'il s'agisse d'un ordinateur portable, d'une tablette ou d'un téléphone, sans surveillance lorsqu'ils travaillent dans un espace de travail public ou n'importe où ailleurs lorsqu'ils sont en déplacement.

Protéger les informations confidentielles – il est toujours bon que les employés protègent les informations confidentielles ou sensibles de leur entreprise de la vue de leur entourage lorsqu'ils travaillent dans des espaces de travail publics. Envisagez de réduire la luminosité de l'écran et de choisir un endroit où l'écran ne peut pas être vu sous n'importe quel angle.

vii. Sécurisation des appareils numériques

Parmi les composants et les outils les plus significatifs et les plus importants au sein de l'écosystème numérique de la vente au détail en pleine évolution, on trouve les différents appareils utilisés pour communiquer, partager des informations et collaborer au travail. Cependant, étant donné que chaque appareil représente une porte d'entrée dans un réseau ou un système, les cybercriminels les ciblent de plus en plus. C'est pourquoi il devient extrêmement important pour les commerces de détail de gérer correctement l'utilisation de ces appareils mobiles et fréquemment utilisés.

Tablettes et téléphones

Les tablettes et les téléphones, qui comptent parmi les appareils les plus couramment utilisés par les commerces de détail et leurs employés, sont malheureusement aussi parmi les objets les plus visés par les vols. Et si une tablette ou un téléphone fourni par un commerce de détail disparaît, il est susceptible d'avoir un certain nombre de conséquences négatives, allant des dommages et de la perte à l'exposition à des maliciels. Pire encore, les informations sensibles et les outils de réseau peuvent être ciblés. Afin d'éviter le pire, les détaillants voudront que leurs employés tiennent compte de certaines choses.

Prose de précautions – il est important que les employés comprennent qu'ils doivent traiter leurs tablettes et leurs téléphones avec le même soin et les mêmes précautions de sécurité qu'ils appliquent à d'autres outils, comme les ordinateurs portables et les ordinateurs personnels.

Accès aux systèmes – les appareils des employés doivent être verrouillés lorsqu'ils ne sont pas utilisés et configurés dans le système du détaillant pour n'être accessibles que par mot de passe.

Sûreté et sécurité – au cours de leurs déplacements, les employés doivent veiller à ce que des mesures de protection appropriées soient mises en place afin de protéger la sécurité des informations sensibles contenues dans les communications.

Stockage portable de données

De nombreux commerces de détail utilisent des dispositifs de stockage de données portables, notamment des disques durs portables et des clés USB. Ils constituent un moyen rapide et facile de transférer des fichiers et des documents volumineux d'un appareil à l'autre. Cependant, ces appareils représentent, une fois de plus, un autre moyen potentiel pour les cybercriminels d'infiltrer les systèmes ou les réseaux d'une entreprise. Par conséquent, les détaillants et leurs employés doivent faire preuve de précaution lorsqu'ils utilisent ces dispositifs.

Utiliser les mesures de protection existantes – la plupart des appareils mobiles sont aujourd'hui équipés de fonctions de sécurité, notamment de logiciels anti-maliciel, qui doivent être activées sur chaque appareil fourni par l'entreprise.

Assurer le cryptage – tous les dispositifs de stockage de données portables doivent être cryptés.

viii. Sécurisation de l'espace physique

Les couches de protection qui seront mises en place pour sécuriser l'activité numérique du commerce de détail, comme l'authentification et le cryptage, sont évidemment nécessaires, mais les aspects physiques critiques de la sécurité ne peuvent pas être oubliés afin de garantir l'efficacité maximale des efforts de cybersécurité d'un détaillant.

Hors de vue – lorsque les employés ne sont pas à leur poste de travail, les dossiers, documents, CD, clés USB ou tout autre objet contenant des données et informations sensibles ou confidentielles doivent être rangés et mis hors de vue.

Verrou – les employés doivent toujours désactiver leur ordinateur lorsqu'ils quittent leur poste de travail. Cette opération peut être effectuée dans la plupart des systèmes en entrant une combinaison de touches. Un mot de passe sera requis pour réutiliser l'ordinateur.

Éviter d'avoir un « bureau en désordre »

Il existe des erreurs de type « bureau en désordre » commises par les employés. Elles sont à éviter pour limiter la cybercriminalité.

Laisser les écrans d'ordinateur allumés sans protection par mot de passe – n'importe qui a donc accès au système. Veillez à verrouiller les paramètres de l'écran.

Placer sur le bureau des documents susceptibles de contenir des informations sensibles – il est préférable de conserver ce type de documents sous clé dans des tiroirs ou des classeurs.

Oublier de déchiqueter les documents avant de les jeter à la poubelle ou au recyclage – tout document peut contenir des informations sensibles. Il est préférable de toujours déchiqueter les documents.

Ne pas fermer les classeurs – il est ainsi plus facile pour quelqu'un de voler des informations sensibles et plus difficiles de se rendre compte qu'un vol a eu lieu.

Laisser les téléphones et les clés USB à portée de tous – ces appareils contiennent sans doute des informations professionnelles ou personnelles sensibles et ils sont faciles à prendre sans que personne ne s'en rende compte.

Oublier d'effacer les notes sur les tableaux – souvent, ces tableaux affichent des informations confidentielles concernant des produits, des idées nouvelles et des processus commerciaux exclusifs.

Laisser un sac à dos sans surveillance – il y a souvent au moins un appareil ou un dossier contenant des informations sensibles dans un sac à dos.

Inscrire les noms d'utilisateur et les mots de passe sur des bouts de papier – il est d'autant plus important d'éviter cela, car ces renseignements peuvent souvent servir à accéder à plusieurs sites.

Laisser la clé d'un tiroir fermé à clé sur place – il est ainsi beaucoup trop facile pour quelqu'un de revenir plus tard, éventuellement après les heures de travail, lorsque personne n'est présent, et d'accéder à des dossiers confidentiels.

Affichage des calendriers au vu et au su de tous – les calendriers contiennent souvent des dates sensibles et/ou des informations sur les clients (existants ou potentiels) ou les nouveaux produits. Conservez-les dans un dossier ou à l'abri des regards.

Laisser les portefeuilles et les cartes de crédit sur le bureau – il s'agit principalement d'un problème pour l'employé, mais un portefeuille peut aussi contenir des cartes de crédit de l'entreprise et des badges de sécurité.

Dans le monde d'aujourd'hui, où les employés sont toujours en déplacement, trop de temps est nécessaire pour déterminer si des documents, des clés USB, des appareils et d'autres éléments contiennent ou non des informations sensibles. La pratique la plus sûre consiste à s'assurer que tout est classé, détruit ou mis sous clé.

ix. Ressources pour les détaillants

Voici une liste de ressources pour aider les commerces de détail à mieux se protéger contre la cybercriminalité :

Programme Cybersécurité au détail du CCCD :
https://www.commercedetail.org/programme-cybersecurite-au-detail-du-cccd/

Centre canadien pour la cybersécurité :
https://www.cyber.gc.ca/fr

Centre canadien pour la cybersécurité – Alertes et avis :
https://www.cyber.gc.ca/fr/alertes-avis

Centre antifraude du Canada :
https://antifraudcentre-centreantifraude.ca/protect-protegez-fra.htm

Gouvernement du Canada – Cybersécurité :
https://www.canada.ca/fr/services/defense/cybersecurite.html