CONSEIL CANADIEN DU COMMERCE DE DÉTAIL

CYBERSÉCURITÉ AU DÉTAIL

MODULE 2

CYBERSÉCURITÉ POUR LES DÉTAILLANTS

Protégez vos équipes, vos dispositifs, vos biens et votre entreprise.

Un guide pour aider les détaillants à protéger leurs équipes et leur entreprise 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

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

La gestion d'une entreprise spécialisée dans le commerce de détail a traditionnellement requis un important degré de détermination et de travail pour assurer l'obtention de résultats satisfaisants. Cependant, la qualité la plus importante qu'un détaillant doit posséder est, sans aucun doute, la capacité et le désir d'évoluer et de s'adapter aux tendances qui sont en constant changement, aux goûts et comportements des consommateurs, aux normes et règlements en matière d'emploi, aux préférences des employés en matière de travail et bien plus encore. Le détaillant doit, en plus de cela, diriger l'ensemble de son entreprise, en attribuant et en gérant les responsabilités liées au personnel et en procédant au suivi du rendement global de chaque employé et de l'entreprise en général.

De nos jours, les évolutions les plus récentes et les fonctions de contrainte de l'industrie, principalement motivées par la numérisation du monde qui nous entoure, font que les détaillants doivent assurer le maintien de la sécurité numérique de leurs opérations et aider leur personnel à protéger l'entreprise contre les menaces posées par la cybercriminalité. Et, étant donné la croissance de cette cyber-criminalité, le nombre et la gravité des cyberattaques lancées contre des entreprises sans méfiance décuplent chaque jour. En ciblant des sites Web, des adresses électroniques, des comptes de réseaux sociaux et tout autre actif numérique associé à une organisation de commerce de détail, les cybercriminels espèrent recueillir, par tous les moyens à leur disposition, de l'information professionnelle ou personnelle sensible et de valeur. Notons, en outre, que la fréquence de ces attaques augmente. Selon une récente étude de Mastercard, la cybercriminalité a bondi de 600 % et les cyberattaques de 238 % depuis le début de l'année 2020.

Au vu de cette inquiétante tendance, et afin d'aider les détaillants à se préparer personnellement et à préparer leurs employés au mieux pour atteindre et maintenir un niveau élevé de sécurité dans leur environnement numérique, le Conseil canadien du commerce de détail (CCCD) a préparé un guide sur la cybersécurité pour les détaillants. Ce guide contient une multitude de renseignements pratiques, de suggestions, de recommandations et de meilleures pratiques et a été conçu pour servir de source et de référence aux commerçants pour les aider à protéger leurs employés et leur organisation contre les menaces que présente la cybercriminalité.

Conséquences de la cybercriminalité :

- Le coût moyen d'un incident de violation de données au Canada est de 5,64 M$– 1 M$ de plus que les moyennes mondiales –, 99 % des victimes indiquent que l'attaque a eu des répercussions sur leurs opérations*.
- La conséquence la plus courante d'un incident de violation de données citée par les détaillants est la perte de données clients. Un tiers des détaillants ont indiqué que l'attaque avait nui à la relation entre les fournisseurs et les clients*.
- Seulement en 2022, la cybercriminalité et la fraude ont coûté plus de 500 M$ aux Canadiens**.
- Chaque année, 24 % des cyberattaques ciblent les commerces de détail – de tous les secteurs, celui du détail est le plus visé***.
- Lors d'une attaque, 42 % des données compromises sont liées au paiement, et 41 % sont des renseignements qui permettent l'identification d'une personne****.

** Selon l'étude sur la sécurisation de l'économie numérique de Mastercard*

*** Selon des données de la GRC*

**** Selon Trustwave **** Selon Verizon*

ii. Évaluer les menaces et les risques en matière de cybersécurité

Une grande partie des responsabilités des détaillants concernant le maintien de la politique de sécurité d'une organisation est de reconnaître et de classer par ordre de priorité une vaste gamme de menaces à la cybersécurité et les risques connexes pour leur entreprise. Ces gestionnaires devront également développer un plan de sécurité détaillé et complet qui constituera un des fondements de la stratégie de l'organisation. Ce plan devra être mis à jour et être utilisé régulièrement comme référence et constituera une des bases de la formation et de la sensibilisation en matière de sécurité de l'organisation pour les employés.

Définir et classer par ordre de priorité

Avant de définir les outils et les pratiques nécessaires pour assurer la sécurité de l'environnement numérique d'une organisation de commerce de détail, les détaillants devront aider à déterminer les menaces à la cybersécurité auxquelles leur organisation risque de faire face et les risques qui peuvent en découler.

Une fois que les menaces et les risques connexes auront été identifiés, les détaillants devront les classer par ordre de priorité en se basant sur un certain nombre de facteurs, y compris la probabilité que l'événement se produise, ainsi que la nature et la gravité des risques connexes. Ces menaces peuvent être classées dans les catégories suivantes : Risque faible, Risque moyen, Risque élevé.

Développer un plan

Lorsque les détaillants auront identifié les menaces et les risques connexes, ils devront développer un plan de cybersécurité complet qui répertorie les politiques, les procédures et les protocoles et qui mette de l'avant les mesures de sécurité, les outils et les ressources appropriés pour atténuer les menaces et limiter tout risque pour l'entreprise.

Ce plan devra définir clairement les rôles et les responsabilités des employés au sein de l'organisation, ainsi que les mesures à prendre pour assurer la sécurité de l'organisation.

Il est recommandé que, quelle que soit la taille de l'organisation, un membre de l'équipe de direction soit nommé pour s'assurer du rendement du plan de cybersécurité, ce qui inclut la mise en œuvre et la mise à jour des outils et le respect de la conformité aux normes, aux meilleures pratiques et au budget alloué pour les ressources.

Sensibilisation des employés

La direction devra s'assurer que tous les employés de l'organisation aient une connaissance approfondie de l'information contenue dans le plan sur la cybersécurité et qu'ils la revoient de manière régulière, pour acquérir une compréhension approfondie des politiques, des procédures et des outils qui ont pour objet de protéger l'intégrité numérique de l'organisation.

iii. Gérer la cybersécurité

Lorsque l'organisation aura déterminé qu'elle a bel et bien besoin d'un plan de cybersécurité formel et compréhensif pour se protéger contre les menaces à la cybersécurité, elle devra prendre des mesures pour créer le plan et développer les politiques, procédures et outils qui seront inclus et mis de l'avant dans le plan et désigner les personnes qui participeront activement à la mise en œuvre du plan.

Développer des politiques et des normes

Afin de pouvoir créer un bon plan de cybersécurité, il est nécessaire de développer un ensemble de politiques, de procédures et de protocoles solides qui définissent et expliquent clairement ce que les employés doivent et ne doivent pas faire pour assurer la cybersécurité de l'entreprise. La direction joue un rôle essentiel dans le développement de ces politiques et procédures et est responsable de l'adhésion des employés à ces politiques, procédures et protocoles.

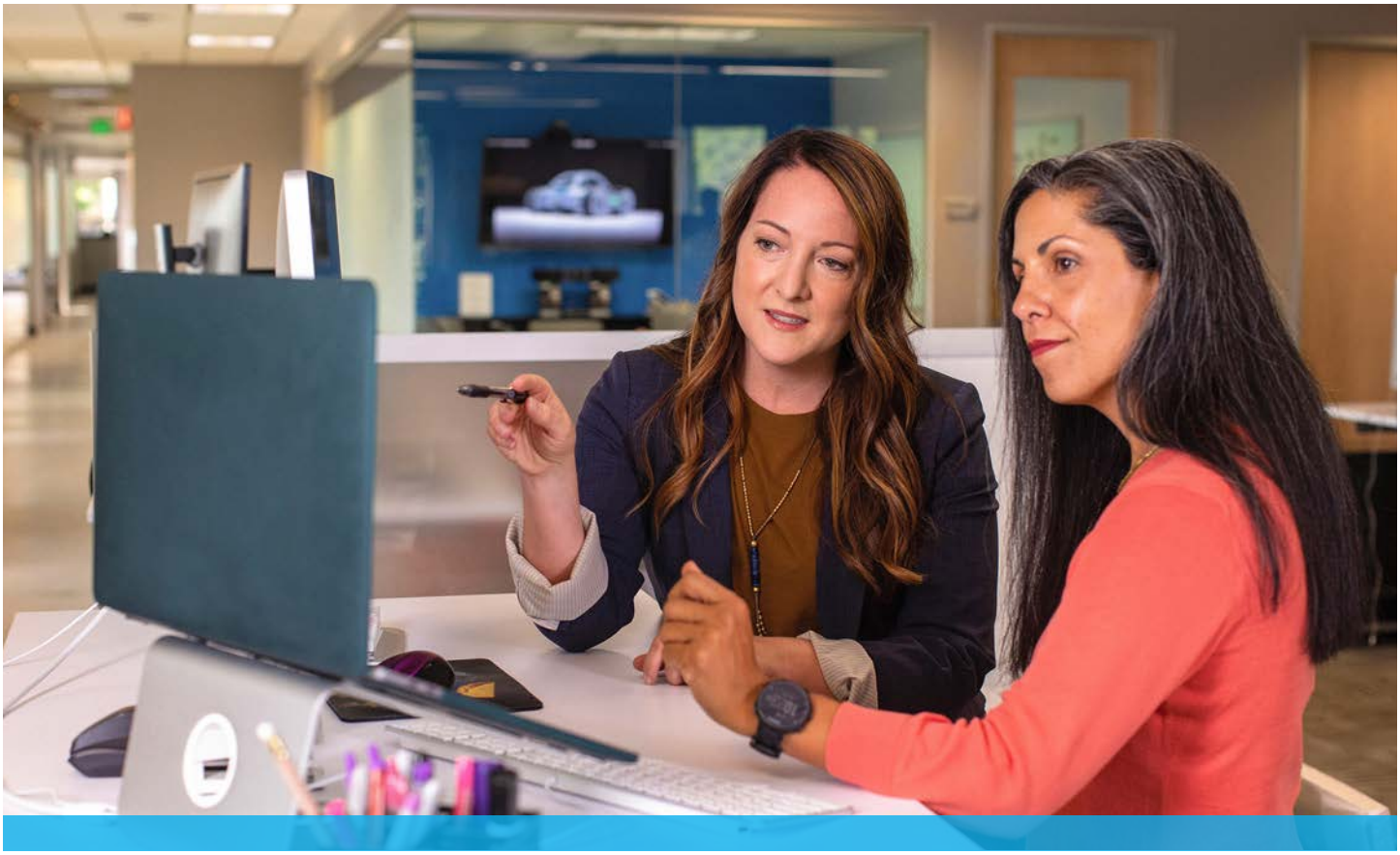
Le plan de cybersécurité devra inclure des politiques liées, entre autres, à l'usage d'Internet, à l'utilisation des réseaux sociaux, au traitement de l'information, à l'usage approprié des dispositifs mobiles et des ordinateurs et aux communications à distance. Un plan de cybersécurité a deux objectifs essentiels : 1) la protection des biens, des employés et des clients de l'organisation ; et 2) la création de normes qui guideront les opérations dans le domaine et le paysage numériques, ce qui permettra de réduire le risque d'erreurs internes.

On pourra développer les normes établies au sein du plan de protection de la cybersécurité en documents de procédure opérationnelle standard afin de les mettre encore davantage en évidence. Ces documents pourront être consultés et utilisés comme référence par les employés de manière régulière.

Au moment de développer des politiques et des procédures de cybersécurité propres à leur organisation, les détaillants devraient tenir compte des points suivants :

Faire simple dans un premier temps – Il est préférable de commencer par mettre au point un plan de cybersécurité relativement basique contenant des politiques et des procédures fondamentales, auxquelles viendront ensuite s'ajouter des renseignements plus détaillés et complexes.

Cerner et adapter les normes existantes – Au moment de développer un plan de cybersécurité, les gestionnaires s'attacheront à y intégrer le plus grand nombre possible de politiques et de procédures efficaces existantes afin de préserver l'uniformité opérationnelle et de lever toute incertitude.



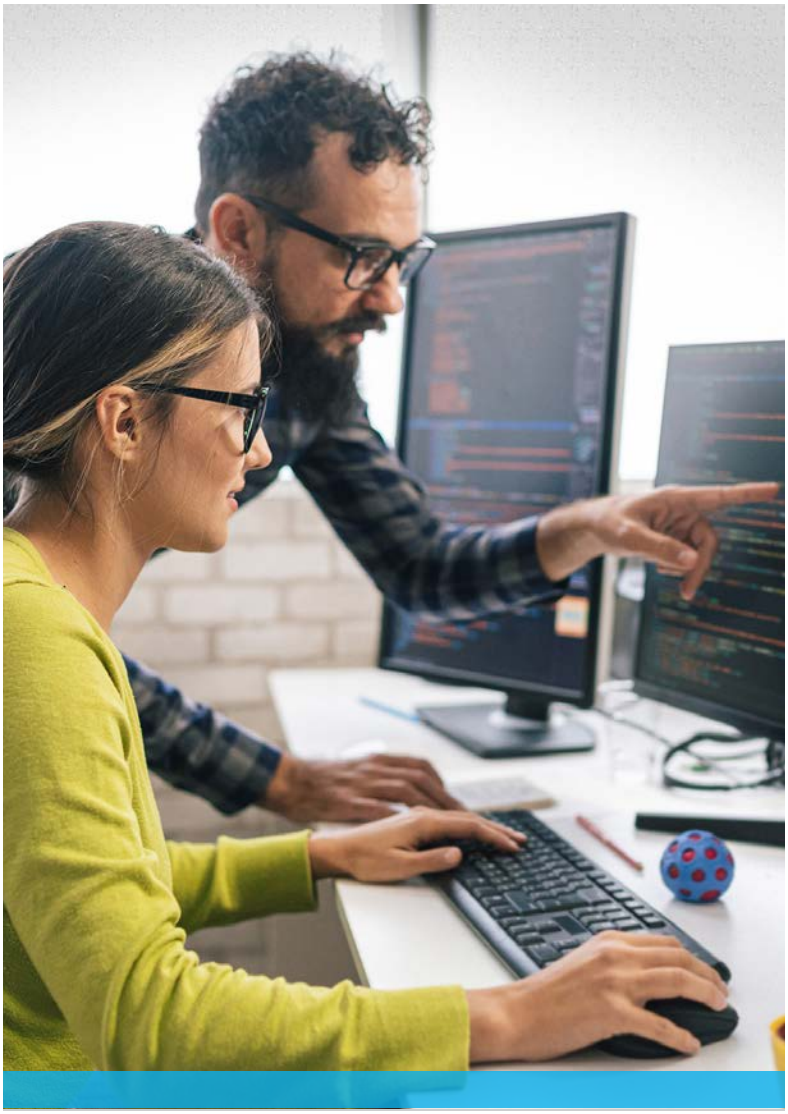
Expliquer le raisonnement – Pour que les politiques et les procédures soient les plus efficaces possible, il faut que les employés comprennent les raisons pour lesquelles elles sont en place et la manière dont elles contribuent à protéger l'entreprise, ses actifs, ses employés et ses clients.

Relire, réétudier et réviser – Comme dans le cas de presque tous les autres documents existants, chaque détaillant doit régulièrement réétudier son plan de cybersécurité, et le réviser au besoin.

Attribuer les rôles et les responsabilités

Après avoir mis le plan de cybersécurité en place, il sera temps d'attribuer des rôles et des responsabilités spécifiques à diverses personnes. Chaque tâche énumérée ci-dessous devra être assumée par une personne :

- Promotion de la sensibilisation aux tendances, menaces et risques connexes pour l'entreprise
- Connaissance et mise en œuvre d'outils de sécurité de pointe, au besoin
- Responsabilité de la sensibilisation et de l'éducation en matière de cybersécurité au sein de l'organisation
- Respect par tous les employés des politiques, des procédures et des meilleures pratiques en matière de cybersécurité
- Révision et mise à jour régulières des outils et des mesures de protection des outils de cybersécurité



Il est évident que, malgré le haut degré d'expertise et les connaissances utilisées pour établir le plan de cybersécurité, le soutien de la direction sera nécessaire au moment de l'exécution de ce plan et de la mise en œuvre des meilleures pratiques. Ce soutien se présentera sous la forme de conseils et de recommandations sur les activités liées à la cybersécurité à tous les employés, une participation active à divers projets liés à la cybersécurité et la collaboration avec des experts externes, y compris avec des conseillers juridiques, quand cela sera nécessaire.

Améliorer la sensibilisation en matière de sécurité

Afin de s'assurer que le plan et toutes ses politiques et procédures aient le plus grand impact au sein de l'organisation, il sera essentiel de promouvoir la sensibilisation et l'éducation en matière de cybersécurité et de mettre l'accent sur son importance.

La direction pourra inclure des ressources et des matériaux éducatifs sur les différentes menaces et les risques qui y sont associés dans le programme de sensibilisation à la cybersécurité, en complément du plan de cybersécurité de l'entreprise.

Le programme de sensibilisation sur la cybersécurité devrait être géré par la direction et inclure tous les employés travaillant dans la vente au détail au sein de l'organisation. Les formations et séances éducatives devraient se faire en groupe pour permettre le renforcement de l'esprit d'équipe et de collaboration des employés et le renforcement approprié et efficace des politiques et des procédures normalisées.

Les formations et les séances éducatives pourraient s'accompagner de jeux-questionnaires, de concours et de récompenses, ce qui permettrait à la direction de communiquer de l'information essentielle en matière de sécurité de manière à ce qu'elle soit comprise et intégrée par les employés.

iv. 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 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 biens doit être adoptée.

Renseignements personnels et professionnels

Il existe un certain nombre de situations au sein d'une entreprise de détail 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. 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 biens 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 présente 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 considérablement réduite 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 dispositifs informatiques de l'organisation comprennent l'importance de ne visiter que des sites Web légitimes et de confiance.

Vérification du destinataire – Avant de communiquer des informations personnelles ou professionnelles à qui que ce soit, les employés doivent s'assurer que le destinataire ne présente aucun risque.

Questions – Chaque fois que quelqu'un demande des informations personnelles ou professionnelles, les employés doivent lui demander les raisons pour lesquelles ces informations sont nécessaires. Si la réponse fournie n'est pas satisfaisante, les employés doivent refuser de fournir les informations demandées jusqu'à réception de nouveaux détails.

Maintien des mesures de protection – Malgré les raisons qui peuvent être invoquées, rien 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.

Pratiques liées à Internet

Les détaillants et leurs employés dépendent énormément d'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 Internet. Bien que l'utilisation d'Internet soit aujourd'hui généralisée, 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 d'Internet à l'interne, qui explique clairement aux employés ce qu'il faut faire et ne pas faire en matière de connexion à Internet à partir des systèmes et des dispositifs de l'entreprise.

Formation des employés – Après avoir élaboré des politiques encadrant l'utilisation d'Internet par les 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 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.

Protocoles liés aux 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 groupe de personnes qui seront responsables de l'activité de l'organisation sur 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 peut être saisi sur les réseaux sociaux. Cela peut être inclus dans la politique d'utilisation d'Internet.

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

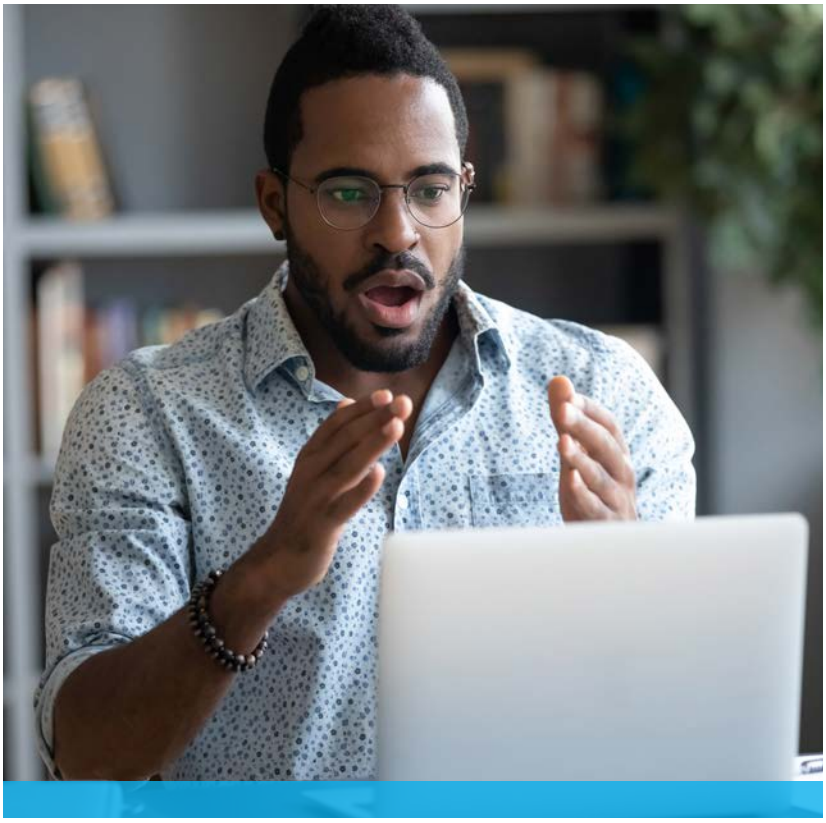
Se méfier des applications de réseautage – Il est judicieux que les entreprises de vente au détail et leurs employés évitent d'utiliser les applications de réseautage, qui sont souvent créées et gérées par des tiers et qui ne sont donc pas forcément aussi sécuritaires que les sites Web correspondants.

Faire preuve de prudence dans les communications – Lorsqu'ils communiquent avec quelqu'un sur des sites de réseaux sociaux, les employés d'un 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 lorsqu'on communique sur les 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. Dans ce cas, les gestionnaires doivent leur demander de mettre en œuvre les mêmes recommandations et d'observer les meilleures pratiques en la matière.

Se protéger contre le piratage psychologique



Les moyens de perpétrer des cyberattaques se multiplient, tout comme les manipulations avec lesquelles elles sont déployées. 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 aux renseignements qu'ils contiennent.

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 comme 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 que ces dernières 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 dans leurs communications avec les sources extérieures.

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 – Il est bon de confirmer l'identité de toute personne requérant un certain type d'information en demandant l'accès à 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.

Sécuriser les logiciels

Même si la direction développe un grand nombre de meilleures pratiques ou offre des formations ou des séances d'éducation à ses employés, un programme de protection de la cybersécurité ne peut pas être plus efficace que le logiciel utilisé pour protéger l'organisation. Des fonctionnalités et des mesures de protection solides assurant la protection des logiciels déployés au sein d'une organisation peuvent servir à atténuer et à éliminer un grand nombre de menaces à la cybersécurité.

Malheureusement, les logiciels généralement installés sur les bureaux d'ordinateur et les applications de dispositifs mobiles, les serveurs Web et les systèmes d'exploitation contiennent ou développent souvent des bogues qui peuvent créer des vulnérabilités et les rendre moins sécuritaires, et donc plus vulnérables aux attaques des cybercriminels. En outre, les logiciels peuvent être infectés par un maliciel.

Afin d'éviter tout problème de sécurité lié au logiciel utilisé par une organisation, la direction devrait collaborer avec le service des TI pour assurer le maintien de la sécurité du logiciel en procédant comme suit :

Utiliser un logiciel légitime – Il est essentiel que la direction s'assure que l'organisation utilise un logiciel légitime. Elle devrait, en outre, s'assurer que ce logiciel a été testé et utilisé par d'autres avant de l'utiliser. Et surtout, **N'UTILISEZ PAS** de version non autorisée d'un logiciel– ces versions sont souvent corrompues ou infectées et peuvent causer de graves dommages aux systèmes de votre organisation.

Limiter l'accès – La direction devrait limiter l'accès aux applications partagées aux personnes qui en ont besoin pour exécuter leur travail et s'acquitter de leurs responsabilités. En outre, le nombre d'employés à qui on a octroyé des privilèges administratifs devrait également être géré pour que les points vulnérables de l'organisation soient réduits au minimum, tout comme les cibles potentielles de cyberattaques.

Procéder régulièrement à des mises à jour – Il est important de s'assurer que toutes les mises à jour, souvent appelées « corrections », soient effectuées dès qu'elles sont disponibles.

Hébergement et cybersécurité de l'entreprise

Un autre secteur de l'écosystème numérique de l'entreprise vulnérable aux attaques est son site Web. Si le site n'est pas sécurisé de manière appropriée, il peut être la cible de cybercriminels qui cherchent à profiter de l'occasion.

Les entreprises hébergent leur site Web de diverses façons. Selon les préférences de votre organisation, voici quelques recommandations utiles.

Hébergement sur des serveurs internes :

Accès restreint – Accès aux employés autorisés uniquement.

Mise en œuvre des mises à jour – Il est important de travailler avec le service des TI pour s'assurer que toutes les mises à jour ont été effectuées dans les systèmes d'exploitation, et ce, pour éviter tout problème ou vulnérabilité.

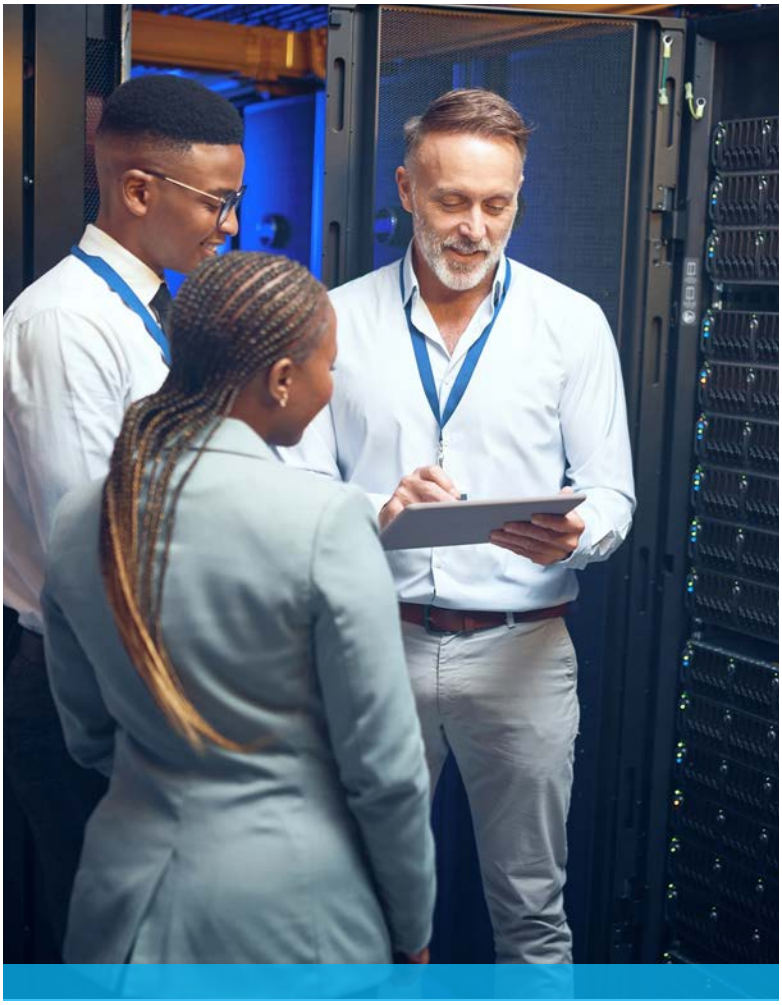
Procéder régulièrement à une sauvegarde – Les gestionnaires devraient s'assurer que les systèmes fassent l'objet d'une sauvegarde régulière, préférablement sur un serveur situé dans un lieu distinct.

Assurer le suivi des registres du serveur – Veillez à ce qu'une personne responsable des serveurs soit nommée et que cette personne procède régulièrement au suivi des registres du serveur pour détecter toute activité suspecte.

Hébergement par le biais d'un service :

S'assurer qu'un plan est en place – La direction devra s'assurer que le prestataire du service dispose de son propre plan de sécurité et que ses meilleures pratiques opérationnelles incluent la numérisation des serveurs Web et de votre site Web pour détecter tout problème potentiel et régler ces problèmes dès qu'ils surviennent, le suivi du site Web de votre organisation et la correction des interruptions ou des lacunes en matière de service causées par l'activité cybercriminelle.

Il est également important que la direction soit préparée au cas où un système serait compromis à la suite d'une cyberattaque, et qu'elle comprenne que les mesures à prendre pourraient inclure de réduire le niveau de service, de passer à un serveur de remplacement, de demander l'aide d'un autre prestataire de services ou, dans le pire des cas, d'éteindre tout le système de manière temporaire. La direction pourra étudier divers scénarios impliquant un serveur compromis afin de préparer un plan permettant de traiter le problème et de déterminer les tactiques à utiliser.



Protection 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 quasi 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 infiltrer d'autres dispositifs. Cependant, il existe d'autres types de maliciels dont les commerces de détail et leurs employés doivent être conscients. En 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.

Rançongiciel – Le cryptage des fichiers sur l'ordinateur d'une victime permet aux cybercriminels 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 de personnes qui ne se doutent de rien.

Logiciel de publicité – Affichage de publicités indésirables sur l'appareil d'un utilisateur. Ce logiciel n'est pas toujours malveillant, mais il 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 et les corrompre ou les supprimer complètement, ce qui permet la collecte illégale d'informations de nature délicate.

Que peuvent faire les détaillants ?

Les maliciels sont souvent incroyablement efficaces, mais les détaillants peuvent prendre certaines mesures pour protéger leurs systèmes professionnels et leurs informations numériques.

Logiciels anti-maliciels – 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-feux – Les détaillants peuvent aussi vouloir installer des pare-feux informatiques afin d'empêcher la connexion à des sites Web malveillants et néfastes. De plus, de nombreux pare-feux sont capables d'empêcher l'intrusion de différents types de maliciels dans le système.

Formation des employés – Parallèlement à la mise en place de logiciels anti-maliciels et de pare-feux, tous les employés de l'entreprise devraient recevoir une formation continue sur la sécurité.

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

Signaler les alertes – Si un employé reçoit un rapport ou un avertissement provenant d'un logiciel anti-maliciels 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 suspectes.

Assurer la mise en œuvre de pratiques d'authentification appropriées

Lorsqu'on traite des volumes importants de données et de renseignements de nature délicate, il est extrêmement important que les pratiques d'authentification mises en place par les détaillants soient respectées 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 aient conscience de l'importance de protéger leurs mots de passe et de ne pas les révéler à 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 toujours 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 de toujours utiliser le même mot de passe pour leurs comptes et sur les différents appareils dont ils se servent.

Modifier fréquemment le mot de passe – Tous les employés doivent fréquemment modifier leurs mots de passe afin de ne pas céder à la complaisance et de les rendre moins prévisibles.

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

Éviter les mots de passe courants 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 comme « 1234 » et des noms personnels faciles à deviner tels que le prénom d'un enfant.

Privilégier les longs mots de passe – 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.

Recourir à des combinaisons – 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 peut 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, « bravoauxchampionsquiloresterontpourtoujours! » devient « brvxchmpnsqlrstrntprtjrs! »), ce qui réduit le nombre de caractères à taper, mais maintient l'efficacité de la protection et de la sécurité.

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

Authentification à deux facteurs

Bien plus difficile à deviner que les mots de passe ou les phrases de passe, l'authentification à deux facteurs permet d'ajouter une couche de complexité et de sécurité aux systèmes des détaillants.

Comme son nom l'indique, l'authentification à deux facteurs exige que la personne ou le système demandant une autorisation d'accès fournisse deux éléments d'authentification. Le premier facteur est 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 deviennent de plus en 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 des détaillants.

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'événement aux forces de l'ordre***
- ***Signaler l'événement au système de signalement des incidents de cybercriminalité et de fraude. Ce signalement sera automatiquement transmis à la Gendarmerie royale du Canada (GRC), au Centre national de coordination en cybercriminalité (CNC3) et au 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.***

v. Sécurisation du système de points de vente

Comme l'écosystème numérique actuel est en constante expansion, il est plus que probable que votre organisation utilise un système de points de vente (PDV) électronique pour exécuter et traiter les transactions financières dans ses magasins. Cette forme de technologie est devenue omniprésente dans les entreprises aujourd'hui, car elle permet aux commerçants d'accepter des paiements par carte de crédit et cartes de débit. Cependant, et comme c'est le cas pour tout ce qui est numérique, les systèmes de PDV peuvent également être des cibles pour les cybercriminels ; les détaillants doivent donc travailler avec le service des TI pour assurer la sécurité des paiements faits par leurs clients.

Pour améliorer la sécurité des systèmes de PDV, les détaillants devront collaborer avec le service des TI pour prendre les mesures suivantes :

S'assurer qu'un pare-feu est en place – Il est essentiel de placer votre système de PDV un pare-feu de sécurité. Il s'agit de l'unique moyen de limiter le trafic entrant et sortant du réseau. Le fournisseur d'accès à Internet de votre organisation/magasin a sans doute installé un pare-feu sur votre routeur, mais il est préférable de vérifier si tel est le cas et de s'assurer de sa fiabilité.

Mettre en place une technique de chiffrement renforcée – Il est extrêmement important d'installer un système de cryptage éprouvé pour la transmission de toutes les données transactionnelles impliquant des détenteurs de cartes entre votre système de PDV et votre fournisseur de services du système de PDV.

Veiller à créer des noms d'utilisateur et des mots de passe uniques – Il est fortement recommandé à votre organisation d'éviter d'utiliser le nom d'utilisateur et le mot de passe par défaut fournis avec votre système de PDV. Ce mot de passe et ce nom d'utilisateurs ouvrent la porte aux cybercriminels qui cherchent la manière la plus facile d'accéder à votre écosystème numérique et à votre organisation.

Limiter l'accès – Votre organisation doit limiter l'accès aux données clients aux personnes qui en ont besoin et qui sont autorisées à les consulter.Effectuer les mises à jour nécessaires – Il est toujours bon de rester à jour en matière de maliciels et de mettre à jour tous les systèmes numériques aussi souvent et aussi régulièrement que possible.

vi. Sécurisation des communications numériques

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

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 les courriels.

Pourriels

Représentant la grande majorité des communications électroniques envoyées sur 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. Le pourriel est incroyablement intrusif et ennuyeux à recevoir. Cependant, quand on clique sur des liens ou ouvre des pièces jointes accompagnant ces envois, des maliciels sont souvent téléchargés sur l'appareil qu'on utilise, 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 doivent veiller à ce que leurs employés soient attentifs aux messages et aux courriels qu'ils reçoivent et qu'ils fassent preuve de prudence pour détecter 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 antipourriels 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 avertisseur.

Formulation maladroite – Le texte peut aussi être formulé de façon maladroite ou inhabituelle, indiquant ainsi que l'expéditeur n'est peut-être pas légitime.

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

Afin de se protéger des répercussions négatives des pourriels, les gestionnaires de commerces de détail devraient sécuriser les listes de courriels de leurs employés et veiller à en assurer la confidentialité. Ils pourraient également envisager d'établir une série de règles et de lignes directrices que les employés devraient suivre au moment de traiter leurs courriels et mettre l'accent sur les recommandations suivantes :

Ne jamais cliquer sur les liens – Les gestionnaires devraient s'assurer que leurs employés sachent qu'ils ne doivent jamais cliquer sur des liens ou des pièces jointes contenus dans un pourriel.

Ne jamais répondre à l'expéditeur – Les employés devraient être informés, quelle que soit la situation, de ne jamais répondre à un pourriel, car cela permettrait de confirmer que l'adresse ou la cible sont réelles et actives.

Effacer – Si un employé est certain qu'un courriel est en fait un pourriel, il doit l'effacer. S'il n'en est pas certain, il doit en informer le service des TI ou son supérieur.

Hameçonnage

Pourriels extrêmement pointus et spécialisés, les courriels d'hameçonnage sont conçus pour ressembler à des messages légitimes 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 caractère, palettes de couleurs et images, et sont impossibles à distinguer d'une communication légitime.

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

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

Intégrer dans les courriels des liens qui redirigent les utilisateurs vers un site Web non sécurisé demandant des informations de nature délicate.

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 de nature délicate.

Usurper l'adresse de l'expéditeur d'un courriel pour faire croire qu'il s'agit d'une source fiable et demander des informations de nature délicate.

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 par 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 courriels sollicitant des informations, y compris en cliquant sur des liens envoyés dans ces courriels.

2. Vérifier la sécurité des sites Web – Il s'agit d'une précaution essentielle à prendre avant d'envoyer des informations de nature délicate sur 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 répondent pas à 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 par 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 prenant l'apparence de sites Web légitimes. L'un des moyens de déterminer si un 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 – Communiquez directement avec l'entreprise dont les courriels semblent provenir. Si un employé reçoit un courriel suspect de la part d'une entreprise connue, comme 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 votre poste 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 de la prévalence des escroqueries par hameçonnage et du 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, communiquez avec 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.

Sécuriser les communications par courriel

La mise en œuvre de mesures de protection contre les pourriels et l'hameçonnage est essentielle, mais il est tout aussi important que la direction éduque les employés sur la manière de sécuriser les communications par courriel, en prenant les mesures suivantes :

Courriels autorisés uniquement – S'assurer que seuls les employés autorisés envoient des courriels à partir de l'entreprise.

Maintien de la confidentialité – Il est important d'enseigner aux employés à protéger la confidentialité de leurs messages électroniques et des pièces jointes à leurs messages jusqu'au moment de les envoyer.

Archivage des courriels envoyés – Il est important que les employés archivent tous les courriels qu'ils envoient, au cas où ces documents devraient servir de références, et ce, pour quelque raison que ce soit.

vii. 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 que ces informations 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 de 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 aux opérations de sauvegarde, 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 de nature délicate

Compte tenu de la quantité de données avec lesquelles les détaillants travaillent régulièrement, au moins une partie d'entre elles peut être considérée comme étant de nature délicate, y compris les informations personnelles des employés, ainsi que les données relatives aux clients et aux finances. La mauvaise manipulation de ces données peut entraîner un accès non autorisé à celles-ci, leur perte, leur exploitation et leur modification, ainsi qu'une série de préjudices pour les entreprises et leurs clients. En conséquence, les employés devraient avoir une connaissance approfondie des meilleures pratiques en matière de traitement des données de nature délicate.

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 de nature délicate, les dossiers et les documents doivent être correctement étiquetés et stockés en conséquence.

viii. 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 cette nouvelle forme de travail par les entreprises partout dans le monde. Le télétravail s'est avéré être un véritable atout pour les entreprises en 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 adoptant des pratiques exemplaires, il est possible d'atténuer une grande part de la menace posée par les cybercriminels.

Les bases du télétravail

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 – Les gestionnaires devraient 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 dispositifs – 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.

Travailler à domicile

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 certaines exigences afin de renforcer la sécurité du travail à domicile.

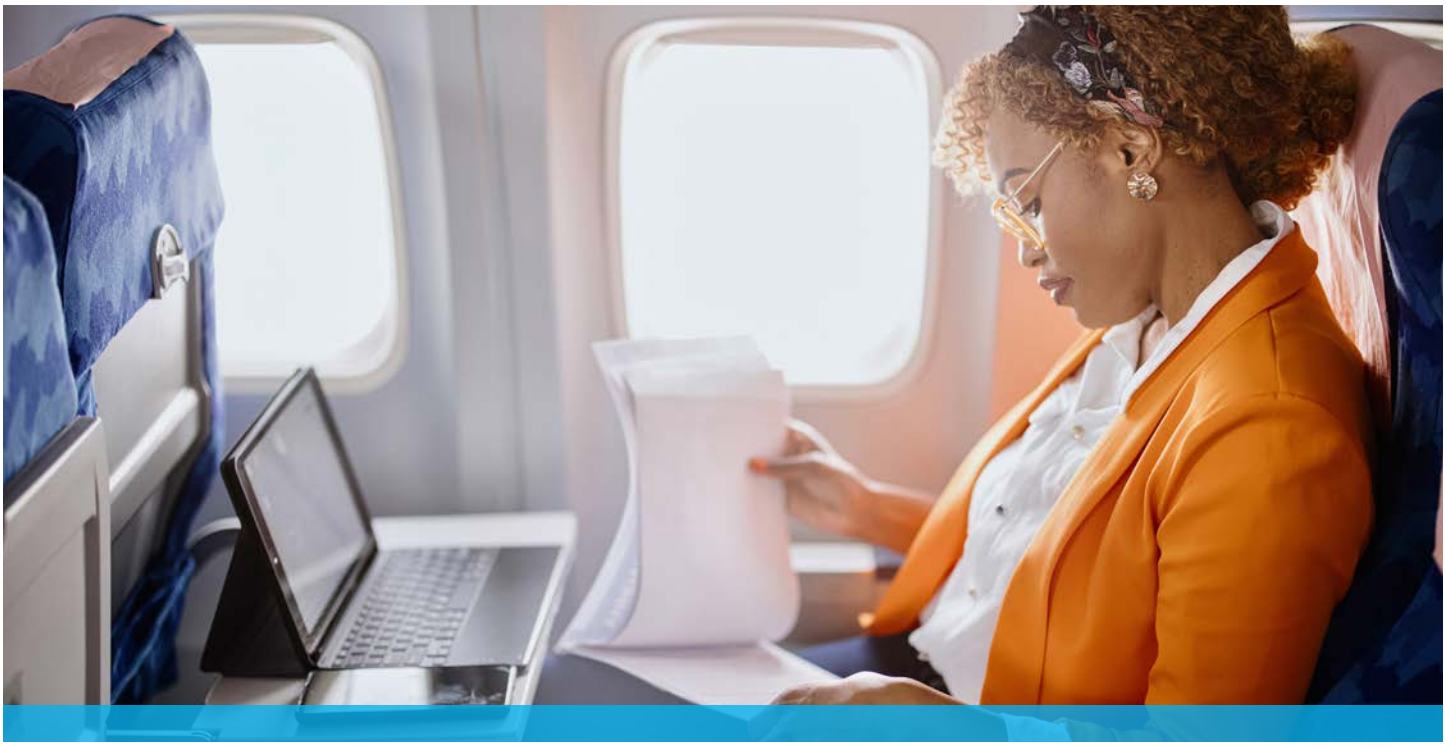
Restrictions de l'accès sans fil – Tous les employés, lorsqu'ils travaillent à domicile sur un ordinateur personnel, doivent connecter leur ordinateur directement à un routeur à l'aide d'un câble Ethernet, et connecter le câble Ethernet au modem, afin d'empêcher toute personne extérieure au réseau d'écouter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

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 leur connexion.

Chiffrement du réseau – Le chiffrement du réseau doit être activé par le service des TI, ce qui permet d'empêcher que les communications et les renseignements de nature délicate soient interceptés et utilisés par des cybercriminels.

Accès limité – En plus des mesures de protection et des 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 qu'ils utilisent pour leur travail.



Travailler pendant les 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 et quand ils se rendent d'un endroit à un autre. 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'elles soient gratuites, elles ne sont souvent pas très sûres.

Gardez vos appareils à portée de main – Les employés en déplacement 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.

Protéger les informations confidentielles – Il est toujours bon que les employés protègent les informations confidentielles ou de nature délicate 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.

Remarque : Toutes les organisations devraient établir une politique obligatoire pour le signalement d'appareils perdus ou volés, et tous les employés devraient consulter cette politique et indiquer qu'ils s'y conforment. Cette politique devrait indiquer diverses façons pour les employés de communiquer avec le service de soutien des TI ou le service d'aide technique à n'importe quel moment.

ix. Sécuriser les appareils numériques

Parmi les composants et les outils les plus importants au sein de l'écosystème numérique de la vente au détail, qui est en pleine évolution, on trouve les différents appareils utilisés pour communiquer, partager des informations et collaborer au travail. Cependant, ceux-ci sont de plus en plus ciblés par les cybercriminels, car ils représentent une porte d'entrée dans un réseau ou un système. C'est pourquoi il devient extrêmement important pour les commerces de détail de gérer correctement l'utilisation de ces appareils mobiles si fréquemment utilisés.

Il revient à la direction de tenir compte des points suivants en ce qui concerne la gestion des appareils numériques et l'atténuation des risques et des inquiétudes en matière de sécurité :

Avantages et inconvénients – Afin de mieux déterminer quels appareils sont indispensables pour l'organisation, il est bon d'établir une liste des avantages et des inconvénients de chacun d'eux.

Appareils approuvés – On pourra, en se basant sur la liste des avantages et des inconvénients, déterminer quels appareils seront autorisés au sein de l'organisation.

Les appareils sont-ils personnels ? – Il est important de déterminer si les appareils mobiles qui appartiennent à une personne sont autorisés ou non au sein de l'organisation.

Établir des règles – Quel que soit l'appareil, il faut établir des règles et les appliquer à tous les appareils et les incorporer dans les procédures d'exploitation qui figurent dans le plan de cybersécurité de l'organisation.

Préparer un plan – Il est recommandé aux détaillants de préparer un plan pour les appareils mobiles, qui comprend les choses à faire et les choses à ne pas faire en matière d'utilisation d'appareils mobiles, car cela leur permet de se protéger de manière efficace contre les menaces que représente la cybercriminalité.

Enregistrer les numéros de série – Il est recommandé d'enregistrer les numéros de série de tous les appareils mobiles utilisés par les employés au sein de l'organisation, car cela sera utile en cas de perte ou de vol.

Afin d'assurer une certaine constance et d'améliorer le niveau de cybersécurité dans une organisation, la direction devrait établir des règles précises sur l'utilisation de chaque appareil.

Tablettes et téléphones intelligents

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 équipements les plus volés. Et si une tablette ou un téléphone fourni par un commerce de détail disparaît, cela peut avoir un certain nombre de conséquences négatives, allant des dommages et de la perte à l'exposition à des maliciels. Pire encore, les informations de nature délicate et les outils de réseau peuvent être ciblés. Afin d'éviter le pire, les détaillants demanderont à leurs employés de tenir compte de certaines choses.

Prise 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 que leurs 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 être configurés dans le système du détaillant pour n'être accessibles que par mot de passe, ce qui permettra de protéger les renseignements de nature délicate, les données et les outils du réseau.

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 de nature délicate contenues dans les communications.

Sauvegardes fréquentes – La direction devra s'assurer que les employés procèdent à la sauvegarde régulière du contenu de leurs appareils.

Utilisation d'applications assurant la sécurité – La direction devra collaborer avec le service des TI pour s'assurer que des applications de sécurité appropriées soient installées et qu'elles offrent des fonctionnalités de cryptage, de localisation des appareils perdus et des anti-maliciels.

Signalement d'une perte – Une procédure devrait être établie pour permettre aux employés de signaler promptement toute perte afin que les forces de l'ordre puissent être informées et tenter de retrouver l'appareil.

Stockage de données portable

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 un autre. Cependant, ces dispositifs 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-maliciels, qui doivent être activés sur chaque appareil fourni par l'entreprise.

Assurer le cryptage – Tous les dispositifs de stockage de données portables doivent être cryptés pour que les renseignements enregistrés sur ces dispositifs soient protégés et sécurisés.

Déterminer les règles – La direction est responsable de déterminer les règles régissant l'utilisation de chacun des appareils utilisés par les employés au sein d'une organisation. On devrait expliquer clairement la nature des renseignements que les employés peuvent stocker sur leurs appareils.

Étiqueter les dispositifs – Il est recommandé d'étiqueter tous les appareils portables de l'organisation. L'étiquette devra comporter le nom de l'organisation et les coordonnées de l'employé qui utilise l'appareil en question, ce qui pourra être utile en cas de perte.

Former les employés – Il est essentiel que les gestionnaires s'assurent que tous les employés soient formés pour assurer le traitement sécuritaire des dispositifs de stockage portables.

x. Sécuriser 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 il ne faudra pas oublier les aspects physiques critiques de la sécurité si l'on tient à garantir l'efficacité maximale des efforts de cybersécurité d'un détaillant.

Assurer la sécurité des employés

La direction assume un rôle et des responsabilités essentiels dans le maintien de la sécurité de l'espace physique du commerce de détail, allant de l'embauche d'employés à l'exécution des tâches quotidiennes.

Afin de s'assurer que l'organisation de vente au détail embauche des employés honnêtes et dignes de confiance, il est important que la direction fasse preuve d'une attention particulière au moment d'embaucher et d'intégrer de nouveaux employés et qu'elle se concentre de manière continue sur les pratiques et le comportement des employés. Voici quelques recommandations destinées à la direction qui lui permettront de s'assurer que les employés comprennent leur rôle au sein de l'organisation :

Préparer une politique de sécurité – Il est essentiel que la direction joue un rôle clé dans l'élaboration, la publication et le maintien d'une politique sur la sécurité qui définisse clairement les règles et les comportements professionnels appropriés dans l'ensemble de l'entreprise ainsi que toute mesure de discipline susceptible d'être appliquée, ce qui inclut le licenciement, si la sécurité de l'organisation a été compromise en raison de la négligence d'un employé.

Procéder à des vérifications d'antécédents – Il est essentiel que les détaillants procèdent à des vérifications approfondies sur les employés potentiels de l'entreprise. Et n'oubliez pas qu'il ne sera pas nécessairement suffisant de vérifier les références fournies, étant donné le niveau de sophistication des activités des cybercriminels.

Établir des règles de non-concurrence – Au moment d'embaucher un employé, la direction devrait très clairement expliquer les règles de non-concurrence et de non-divulgation concernant la propriété intellectuelle et les obligations contractuelles qui peuvent être pertinentes dans le contexte de l'organisation. La direction devrait, par exemple, informer les nouveaux employés qu'il est interdit de divulguer de l'information confidentielle en dehors de l'organisation.

Communiquer les responsabilités – La direction devrait prévoir une formation sur la sécurité, incluant la communication des responsabilités en matière de sécurité dans le processus d'intégration de tout nouvel employé. Cela constitue, en outre, un excellent moment pour présenter la politique sur la sécurité de l'organisation et l'étudier de manière approfondie.

Fin d'accès – Si un employé quitte l'organisation, soit parce qu'il a été licencié, soit parce qu'il a démissionné, il est essentiel que la direction s'assure que l'employé qui quitte l'entreprise n'ait plus accès aux ordinateurs, systèmes, comptes électroniques et à tout autre point de contact numérique, et ce, pour éviter tout problème de sécurité.

Gérer les pratiques des employés

Il est important de noter que les meilleurs efforts d'une organisation en matière de sécurité peuvent être gravement limités si un employé n'est pas pleinement formé et engagé dans le maintien d'un environnement de travail sécuritaire. En conséquence, il est important que la direction soit consciente des erreurs liées à un « bureau en désordre » et qu'elle voie à ce que les employés évitent ce qui suit :

Laisser les écrans d'ordinateur allumés sans protection par mot de passe – N'importe qui peut avoir accès au système si un ordinateur est ouvert. Les employés doivent donc veiller à verrouiller les paramètres de l'écran.

Placer sur le bureau des documents susceptibles de contenir des informations de nature délicate – 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 de nature délicate. 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 de nature délicate et plus difficile 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 de nature délicate et sont faciles à prendre sans qu'on 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 professionnels exclusifs.

Laisser un sac à dos sans surveillance – Il y a souvent au moins un appareil ou un dossier contenant des informations de nature délicate 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 que ces renseignements peuvent souvent servir à accéder à plusieurs sites.

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

Laisser affichés les calendriers au vu et au su de tous – Les calendriers contiennent souvent des dates sensibles ainsi que des informations sur les clients (existants ou potentiels) et 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 un employé, mais un portefeuille peut aussi contenir des cartes de crédit de l'entreprise et des badges de sécurité.

En outre, les gestionnaires devraient s'assurer que leurs employés suivent les meilleures pratiques quand ils ne sont pas à leur bureau. Ces meilleures pratiques incluent :

Rangement – Lorsque les employés ne sont pas à leur poste de travail, les dossiers, documents, CD, clés USB et tout autre objet contenant des données et des informations de nature délicate ou confidentielle doivent être rangés.

Verrouillage – Les employés doivent toujours verrouiller 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.

Limiter l'accès

Il est, en outre, important que la direction de l'organisation limite l'accès à certaines parties de l'espace physique et en accorde uniquement l'accès aux employés qui en ont besoin pour exécuter leurs tâches et s'acquitter de leurs responsabilités. Par exemple, les employés qui travaillent en dehors du service des TI ont rarement besoin d'accéder aux serveurs. Ces zones devraient donc être verrouillées et surveillées pour éviter toute erreur de sécurité.

xi. Quand un soutien est nécessaire

Il n'est pas facile, pour une organisation de commerce de détail, de gérer un programme de cybersécurité pour se protéger de manière efficace contre les menaces que représente la cybercriminalité. Cela est particulièrement vrai pour les entreprises de détail de petite et moyenne taille, qui n'ont pas directement accès à l'expertise nécessaire pour ce faire et aux équipes requises pour mettre en œuvre toutes les initiatives et s'assurer que les meilleures pratiques soient adoptées par le personnel. En conséquence, il est important de comprendre quand et où demander de l'aide pour protéger son entreprise.

Quand demander de l'aide

Un plan de cybersécurité solide comporte de nombreux aspects, y compris la sélection et la mise en œuvre de toute une série de solutions de sécurité, le traitement et la gestion sécuritaires d'une foule de données, la prestation régulière de séances de formation et de séances éducatives au personnel, ainsi qu'une multitude d'autres points essentiels. La gestion d'un tel plan peut donc parfois s'avérer difficile. Si vous pensez que le plan de cybersécurité de votre organisation n'est pas approprié et ne répond pas à tous les besoins connexes de votre entreprise, il est temps de contacter un prestataire de services tiers disposant des connaissances spécialisées nécessaires pour vous aider. Vos besoins en matière de cybersécurité détermineront le style de prestataire que vous contacterez, car il existe de nombreux fournisseurs qui offrent divers services, y compris des services de conseils et des services à la clientèle, qui pourraient être extrêmement utiles à votre organisation.

Protéger votre entreprise

Si votre organisation ne dispose pas des ressources nécessaires pour commencer à développer un programme de cybersécurité complet et efficace, ou si votre budget est limité, vous pourriez utiliser des outils en ligne gratuits. Les commerces de détail devront cependant être prudents au moment de faire des recherches sur ce genre d'outils et s'assurer d'en confirmer la légitimité en vérifiant les sources et les commentaires des utilisateurs. Il est important de comprendre que l'élaboration de tout programme et infrastructure de cybersécurité solide implique au minimum un investissement initial, en plus des paiements réguliers pour les services continus requis. Cela peut sembler coûteux à certains, mais de nombreux prestataires de logiciels de cybersécurité offrent également un soutien aux fournisseurs, des garanties sur leurs produits, un soutien technique pour l'installation et la mise en œuvre ainsi que toute mise à jour qui pourrait être requise ultérieurement.

Quand contacter les autorités

Malgré le nombre d'outils et le soutien technique auxquels une organisation a accès, il arrive qu'il soit nécessaire de contacter les forces de l'ordre. En cas de cyberattaque grave, ce qui peut inclure des menaces ou des dommages aux employés ou aux biens de l'entreprise, les détaillants ne devraient pas hésiter à :

- ***Signaler l'événement aux forces de l'ordre***
- ***Signaler l'incident au système de signalement des incidents de cybercriminalité et de fraude. Ce signalement sera automatiquement transmis à la Gendarmerie royale du Canada (GRC), au Centre national de coordination en cybercriminalité (CNC3) et au 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.***

xii. Auto-évaluation de la cybersécurité

Cette autoévaluation de la cybersécurité est une excellente première étape qui vous aidera, vous et votre personnel, à améliorer vos efforts de sécurité. En prenant connaissance de ces questions et en y répondant avant de lire ce guide dans sa totalité, les gestionnaires de commerces de détail et leurs équipes comprendront mieux l'état de leurs capacités en matière de cybersécurité et, indirectement, quelles parties ou contenu du guide pourraient leur être particulièrement utiles.

Avant de répondre, veuillez noter que ces questions ont été formulées en supposant que votre entreprise, quel que soit sa taille ou son format :

1. utilise des ordinateurs d'entreprise ;
2. utilise des ordinateurs et des appareils de communication portables d'entreprise ;,
3. connecte au moins une partie de ces appareils à Internet au moins une partie du temps ;
4. possède et utilise un intranet afin de diffuser en interne des logiciels d'applications, des documents et d'autres données, de nature délicate ou non.

Pour répondre correctement et de manière précise à cette autoévaluation, veuillez encercler une réponse pour chaque question posée. Si vous ne connaissez pas la réponse, veuillez encercler « Je ne sais pas ».

Questions de l'auto-évaluation de la cybersécurité :

1. La cybersécurité est-elle actuellement une priorité au sein de votre organisation de vente au détail ?

0. Je ne sais pas 1. Non 2. Oui

2. Est-ce qu'un employé de votre organisation de vente au détail est responsable des activités, de la stratégie et du rendement associés à la cybersécurité ?

0. Je ne sais pas 1. Non 2. Oui

3. Si vous avez encerclé « Oui », cette personne occupe-t-elle un poste permanent soutenu par la direction ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

3. Votre organisation de vente au détail a-t-elle déjà effectué une évaluation des risques ou une analyse des menaces, ou tout autre type d'examen semblable ?

0. Je ne sais pas 1. Non 2. Oui

3. Si vous avez encerclé « Oui », les risques et menaces associés ont-ils été classés par ordre de priorité pour tenter de les atténuer ou de les éliminer ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

4. Y a-t-il un plan ou une stratégie de cybersécurité en place au sein de votre organisation de vente au détail ?

0. Je ne sais pas 1. Non 2. Oui

3. Si vous avez encerclé « Oui », les gestionnaires de l'organisation respectent-ils le plan ou la stratégie ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

5. Des politiques de cybersécurité sont-elles en place au sein de votre organisation de vente au détail ?

0. Je ne sais pas 1. Non 2. Oui

3. Si vous avez encerclé « Oui », les politiques sont-elles appuyées par des séances de sensibilisation et de formation continue des employés ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

6. Y a-t-il un plan d'intervention d'urgence en place au sein de votre organisation de vente au détail ?

0. Je ne sais pas 1. Non 2. Oui

3. Si vous avez encerclé « Oui », ce plan est-il tenu à jour et révisé régulièrement ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

7. Votre organisation de vente au détail offre-t-elle à ses employés des séances de sensibilisation et de formation sur le traitement et la désignation sécuritaires des renseignements personnels et/ou commerciaux de nature délicate ?

0. Je ne sais pas 1. Non 2. Oui

3. Si vous avez encerclé « Oui », ces séances de sensibilisation et de formation sont-elles les mêmes pour tous les employés et sont-elles appuyées par des politiques ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

8. Votre organisation de vente au détail offre-t-elle à ses employés des séances de sensibilisation et de formation sur l'utilisation sécuritaire des appareils mobiles ou des ordinateurs ?

0. Je ne sais pas 1. Non 2. Oui

3. Si vous avez encerclé « Oui », cette formation est-elle appuyée par des outils de gestion des appareils mobiles ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

Quelle note avez-vous obtenue ?

Une fois que vous avez rempli le questionnaire, additionnez tous les chiffres situés à gauche des réponses encerclées (0, 1, 2 et 3). Votre note totale vous aidera à évaluer le niveau de cybersécurité au sein de votre organisation et le travail qui pourrait devoir être fait pour améliorer la sécurité de votre entreprise.

Note comprise entre 0 et 7 : Si vous avez obtenu une note dans cette fourchette, nous vous conseillons de bien lire ce guide afin de mieux saisir l'importance d'un plan de cybersécurité solide et complet pour votre organisation. Une fois que vous aurez lu le guide et formulé vos propres recommandations, rencontrez vos collègues et vos supérieurs pour commencer à élaborer et à mettre en œuvre une stratégie de cybersécurité et des outils et procédures connexes.

Note comprise entre 8 et 14 : Si vous vous situez dans cette fourchette, on peut penser que votre organisation a connaissance des risques associés à la cybercriminalité, mais qu'il y a encore du travail et de la recherche à faire. Compte tenu de ce qui précède, il vous est conseillé de lire attentivement l'ensemble de ce guide, en prenant note des domaines dans lesquels des améliorations peuvent être apportées au plan et à la stratégie de votre organisation.

Note comprise entre 15 et 23 : Si vous vous situez dans cette fourchette, félicitations ! Votre organisation semble arriver à maintenir un environnement numérique sécuritaire pour sa marque de détail, ses employés et ses clients. Cependant, compte tenu de la vitesse à laquelle le paysage numérique de la vente au détail évolue, il est toujours bon de continuer à examiner les pratiques exemplaires pour rester au courant des dernières avancées en matière de cybersécurité.

xiii. Ressources pour les détaillants

Pour aider les entreprises de vente au détail à mieux se protéger contre la cybercriminalité, voici une liste de ressources auxquelles vous pourrez accéder et que vous pourrez utiliser en cas de besoin :

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