Lumière sur la
Sécurité
Un guide d'information pour les clients et employés de Securitas Canada

Janvier 2016 | Securitas Canada Limitée | Nombre 142

Dix résolutions de sécurité et de sûreté pour la nouvelle année

Nous devrions profiter du début de la nouvelle année 2016 pour faire table rase et repartir à zéro. La plupart des gens profitent du début de la nouvelle année pour prendre toutes sortes de résolutions et nous-mêmes, à Securitas Canada, vous encourageons à perpétuer cette tradition en prenant des résolutions basées sur la sécurité. Il faut veiller à porter notre attention sur un examen renouvelé de notre sécurité à la fois dans les sphères numériques et physiques. Ces résolutions devraient être appliquées au moins une fois par an et nous rappeler qu'il s'agit d'un procédé constant.

LA SÉCURITÉ NUMÉRIQUE

Nous vivons dans un monde numérique et dépendons de notre interaction avec la technologie et de son utilisation à la fois pour des raisons professionnelles et sociales. Il est important que nous protégions notre monde électronique contre les voleurs éventuels, les pirates informatiques et ceux qui opèrent dans la pénombre cybernétique. Vous devriez vous décider à accomplir cinq tâches dans le cadre des résolutions de sécurité du Nouvel An.

Premièrement, changez les mots de passe de toutes vos connexions numériques. Bien que cela puisse paraître ardu et fastidieux, c'est la garantie que vous avez proactivement une longueur d'avance sur les criminels potentiels. Cela comprend les courriels, toutes vos connexions sur les sites web, les verrouillages d'écran de votre téléphone portable, et même les codes de sécurité à domicile et au travail.

Deuxièmement, vérifiez vos paramètres de confidentialité des médias sociaux. Les applications des médias sociaux sont en évolution permanente et ces compagnies changent constamment leurs programmes et peuvent, au cours d'une mise à jour, exposer vos renseignements «privés» à la vue du public.

Troisièmement, documentez-vous sur les fraudes en lignes les plus récentes et ce que vous devez savoir pour que vos communications électroniques et votre navigation internet soient sécuritaires. L'hameçonnage est un terme général qui s'applique aux courriels, messages texte et sites web inventés par des criminels et conçus pour faire croire qu'ils proviennent de compagnies, d'institutions financières et d'agences gouvernementales réputées et fiables, afin de rassembler des renseignements personnels, financiers et confidentiels. Ce phénomène est aussi connu sous le nom d'usurpation de marque. Assurez-vous que tous vos logiciels, logiciels espions et maliciels sont à jour. Si vous n'êtes pas à jour, vos protections électroniques s'en trouveront affaiblies et vous augmenterez vos risques d'être victime d'une attaque, d'un pirate ou d'un virus. Rappelez-vous, cela s'applique aux ordinateurs, tablettes, téléphones portables et systèmes GPS. Méfiez-vous de tout courriel ou message texte contenant des demandes pressantes de renseignements personnels ou financiers (normalement, les institutions financières et les compagnies de cartes bancaires n'utiliseront pas de courriels pour confirmer les renseignements de leurs clients existants.) En règle générale, n'ouvrez pas les courriels suspects ou qui vous sont parvenus à l'improviste, ne les transmettez pas ou ne cliquez pas dessus (même s'ils proviennent d'un vendeur ou d'un de vos contacts). Méfiez-vous des

fichiers ZIP joints aux courriels. Souvenez-vous que la présence de votre nom ou de votre adresse électronique ne garantit pas l'authenticité de ce courriel. Si vous soupçonnez que votre ordinateur a été infecté, ne vous connectez pas au réseau de votre compagnie ou de votre domicile. Débranchez le cordon de votre réseau et éteignez ou désactivez votre connexion Wi-Fi. Rapportez l'incident immédiatement à l'administrateur de votre réseau.

Quatrièmement, sauvegardez tous vos fichiers électroniques. Cette mesure est recommandée à la fois par l'industrie et par les agences fédérales. Que ce soit dans le nuage ou n'importe quel type de disque dur, lorsque vous possédez une copie de vos fichiers, vous pouvez vous protéger financièrement et professionnellement. Les experts de la sécurité recommandent le format 3-2-1 : trois exemplaires, deux formats différents et un hors-site. Cela garantira aussi qu'au besoin vous aurez accès à des renseignements sauvegardés sous des formats multiples (Rudiments GI – gouvernement du Canada, 2015).

Cinquièmement, lorsque vous vous absentez de votre bureau ou retournez chez vous, éteignez votre ordinateur. De cette façon personne ne peut accéder à distance à votre ordinateur par internet. Dans le même esprit, configurez l'écran de votre ordinateur pour qu'il soit verrouillé s'il est inutilisé pendant plus de deux minutes. De cette façon, si vous vous éloignez de votre bureau ou de votre lieu de travail, personne ne pourra avoir accès à votre ordinateur et aux fichiers confidentiels qui s'y trouvent.

SÉCURITÉ SUR LE LIEU DE TRAVAIL

Après nous être penché sur le domaine numérique, étudions maintenant l'aspect physique de la sécurité sur notre lieu de travail. Il est important de réaliser que l'on peut prendre plusieurs mesures simples pour améliorer notre compréhension des menaces potentielles présentes au bureau. En choisissant nos résolutions du Nouvel An, on peut prendre cinq mesures qui augmenteront notre sécurité physique.

Premièrement, vérifiez que vous comprenez les plans de sortie d'urgence et le système d'alarme d'évacuation du site de votre compagnie. Comprenez les types de plan d'action et les mesures que les employés de la compagnie devront adopter. Sachez aussi qu'à chaque incident peut correspondre une réponse différente. Par exemple, le rapport d'un incendie comparé à une menace à la bombe. Sachez également s'il existe un point de rassemblement à l'extérieur de l'édifice ou si une situation d'urgence exige l'évacuation de tout le site; au cas où il y aurait un point de rassemblement, procédez annuellement à un exercice d'évacuation de l'édifice pour être sûr que tout le monde sache comment procéder et où se rendre.

Deuxièmement, réétudiez vos habitudes lorsque vous arrivez au travail et rentrez chez vous. Utilisez l'entrée principale et évitez les sorties arrières ou isolées. Soyez toujours prudent et conscient de votre entourage lorsque vous vous rendez dans un parc de stationnement. Changez vos habitudes, vos trajets et vos horaires pour éviter d'être prévisible. Essayez de toujours stationner dans des endroits bien éclairés et non près de véhicules dont la grande taille vous obstruerait la vue. Considérez un système de jumelage ou pensez à comment vous rendre à votre automobile en toute sécurité. Ne déverrouillez pas vos portières à distance avant d'être à proximité de votre véhicule et verrouillez-les immédiatement en gardant les fenêtres fermées jusqu'à ce que votre voiture roule. Regardez toujours à l'intérieur du véhicule si vous l'avez laissé déverrouillé avant d'y entrer pour vous assurer que personne ne se cache sur la banquette arrière. Les criminels ciblent les parcs de stationnement et les garages souterrains parce qu'ils offrent de nombreux endroits où se cacher et une façon relativement simple de s'échapper après avoir commis un délit.

Troisièmement, verrouillez la porte de votre bureau ou les tiroirs de votre bureau dans votre cabine chaque fois que vous vous en éloignez. Faites-le au moins quand vous vous éloignez pour une longue période ou pour le reste de la journée. Ce simple geste diminuera les risques qu'un collègue malhonnête ou un vendeur étranger ne fouillent dans les tiroirs de votre bureau pour y chercher des articles de valeur, ou au mieux les en dissuadera.

Quatrièmement, protégez les exemplaires durs des documents et autres matériels confidentiels de la compagnie. Dans le monde moderne de l'espionnage industriel, il est important de protéger les biens internes de la compagnie afin de conserver une longueur d'avance au sein de l'industrie. De même, si les fichiers venaient à être volés, cela pourrait avoir un effet négatif indirect qui conduirait à des pertes de marché et pourrait forcer la direction de l'entreprise à renvoyer du personnel.

Cinquièmement, familiarisez-vous à nouveau avec les politiques des visiteurs de votre compagnie. Connaître l'identité des visiteurs ou des vendeurs et savoir où ils ont la permission d'opérer protégera tout le monde. Sachez aussi qui devrait avoir accès aux sections sensibles de l'édifice. De plus, ne permettez jamais à qui que ce soit d'utiliser vos droits d'entrée dans l'édifice. Si vous remarquez que quelqu'un tente de pénétrer dans l'édifice de cette façon, demandez-lui toujours son numéro d'identification de la compagnie si celui-ci n'est pas visible. Connaître les politiques et le système d'insigne d'identification instaurés par votre compagnie vous permettra d'être plus alerte et de protéger votre compagnie contre les vols et les menaces potentielles.

CONCLUSION

Securitas Canada vous souhaite une bonne année et vous rappelle que la vigilance est une valeur qui doit être ravivée en permanence. C'est grâce à cette approche proactive et l'examen de notre sécurité électronique ainsi que de celle de nos lieux de travail que nous pourrons être protégés et rester en sécurité tout au long de l'année qui s'en vient. **Nous vous souhaitons une année 2016 heureuse et sécuritaire!**