



Trousse de sensibilisation en cybersécurité

En collaboration avec



Licence et Avertissement



Sujet au respect des termes et conditions de cette licence, Cybereco vous octroie le droit gratuit et non-exclusif d'utiliser et de reproduire ce matériel à des fins internes ainsi que de le partager selon les mêmes termes et conditions. Le matériel ne peut être modifié et la marque de Cybereco et les termes et conditions de cette licence doivent y demeurer apposés tels quels.

Cette licence ne vous permet pas de revendiquer quelque droit de propriété intellectuelle dans le matériel, de le vendre ou d'utiliser toute marque de commerce qui y est contenue séparément sans l'autorisation de son propriétaire.

LES RENSEIGNEMENTS CONTENUS DANS CE MATERIEL SONT D'ORDRE GÉNÉRAL SEULEMENT ET NE CONSTITUENT PAS DES CONSEILS OU DE SERVICES PROFESSIONNELS. AVANT DE PRENDRE UNE DÉCISION OU DE PRENDRE DES MESURES QUI POURRAIENT AVOIR UNE INCIDENCE SUR VOS FINANCES OU VOS ACTIVITÉS, VOUS DEVRIEZ CONSULTER UN CONSEILLER PROFESSIONNEL QUALIFIÉ.

CE MATERIEL EST MIS À VOTRE DISPOSITION « TEL QUEL » ET SANS AUCUNE GARANTIE. SANS LIMITER LA PORTÉE DE CE QUI PRÉCÈDE, CYBERECO NE GARANTIT PAS QUE LE MATERIEL PUISSE ÊTRE UTILISÉ CONFORMÉMENT À L'USAGE AUQUEL IL EST DESTINÉ, QU'IL NE CONTIENT AUCUNE ERREUR, NI AUCUN VIRUS OU PROGRAMME MALVEILLANT, NI QU'IL RÉPOND À DES CRITÈRES PRÉCIS EN MATIÈRE DE SECURITÉ, DE RENDEMENT OU DE QUALITÉ. TOUTE GARANTIE IMPLICITE DE QUALITÉ MARCHANDE, DE CARACTÈRE APPROPRIÉ À UNE FIN DONNÉE, DE TITRE ET À L'ABSENCE DE VIOLATION DE DROITS DE PROPRIÉTÉ INTELLECTUELLE, À LA COMPATIBILITÉ, À LA SÉCURITÉ ET À L'EXACTITUDE EST EXPRESSÉMENt REJETTÉE.

Licence et Avertissement



L'UTILISATION DE CE MATERIEL EST À VOS PROPRES RISQUES, ET C'EST À VOUS D'ASSUMER LA PLEINE RESPONSABILITÉ ET DE TOUTE PERTE RÉSULTANT DE CETTE UTILISATION, Y COMPRIS, SANS S'Y RESTREINDRE, TOUTE INTERRUPTION DE SERVICES OU PERTE DE DONNÉES. NOUS N'ASSUMERONS AUCUNE RESPONSABILITÉ À L'ÉGARD DE DOMMAGES-INTÉRÊTS DIRECTS, INDIRECTS, SPÉCIAUX, ACCESSOIRES, CONSÉCUTIFS OU PUNITIFS, NI D'AUCUN AUTRE DOMMAGE QUEL QU'IL SOIT, QUE CE SOIT DANS UNE ACTION EN JUSTICE RECHERCHANT UNE RESPONSABILITÉ CONTRACTUELLE, JURIDIQUE OU DÉLICTUELLE (Y COMPRIS, SANS S'Y RESTREINDRE, LA NÉGLIGENCE) OU AUTREMENT, RELATIVEMENT À L'UTILISATION DE CE MATERIEL MÊME SI NOUS ÉTIONS, OU AURIONS DÛ ÊTRE, AU COURANT DE LA POSSIBILITÉ DES DOMMAGES.

CERTAINS LIENS DE CETTE TROUSSE FONT RÉFÉRENCE À DES SITES WEB OU ARTICLES QUI NE SONT PAS SOUS LE CONTRÔLE DE CYBERECO. CYBERECO N'EST PAS RESPONSABLE DU CONTENU DE CES SITES WEB, NI DES INFORMATIONS, LOGICIELS, PRODUITS ET SERVICES DISPONIBLES SUR OU PAR L'INTERMÉDIAIRE DE CES SITES. LES LIENS SÉLECTIONNÉS SONT UNIQUEMENT DESTINÉS À FOURNIR UN COMPLÉMENT D'INFORMATION. CYBERECO N'ASSUME AUCUNE OBLIGATION OU RESPONSABILITÉ DE QUELQUE NATURE QUE CE SOIT À CET ÉGARD.

CETTE EXONÉRATION DE RESPONSABILITÉ VAUT POUR CYBERECO ET CHACUN DES MEMBRES CYBERECO AINSI QU'À NOTRE PERSONNEL, NOS CONSULTANTS ET À LEUR PERSONNEL ET LEURS CONSULTANTS RESPECTIFS.

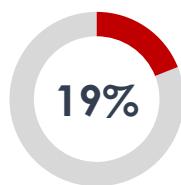


Contexte de la cybersécurité

La cybersécurité



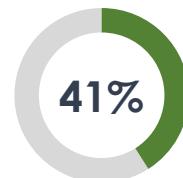
Véritable enjeu de ces dernières années et des années à venir, la cybersécurité est l'affaire de tous, et nul n'est épargné par les cyber attaques. Bien que seules les attaques visant de grosses entreprises soient médiatisées, les entreprises de taille plus modeste sont elles aussi victimes des cybercriminels. En effet, voici quelques chiffres représentant le pourcentage des entreprises touchées, selon la taille de l'entreprise* :



Petite taille
(10 à 49 employés)



Taille moyenne
(50 à 249 employés)



Grande taille
(250 employés ou plus)

De plus, selon une étude réalisée en 2017 sur un échantillon de 12 000 entreprises canadiennes, **21%** des entreprises ont déclaré qu'elles avaient été **touchées** par un incident de cyber sécurité, qui a eu des répercussions sur leurs activités.

* Source: <https://www.desjardins.com/ressources/pdf/f20-etat-de-la-cybersecurite-des-entreprises-canadiennes-f.pdf?resVer=1560872566000>

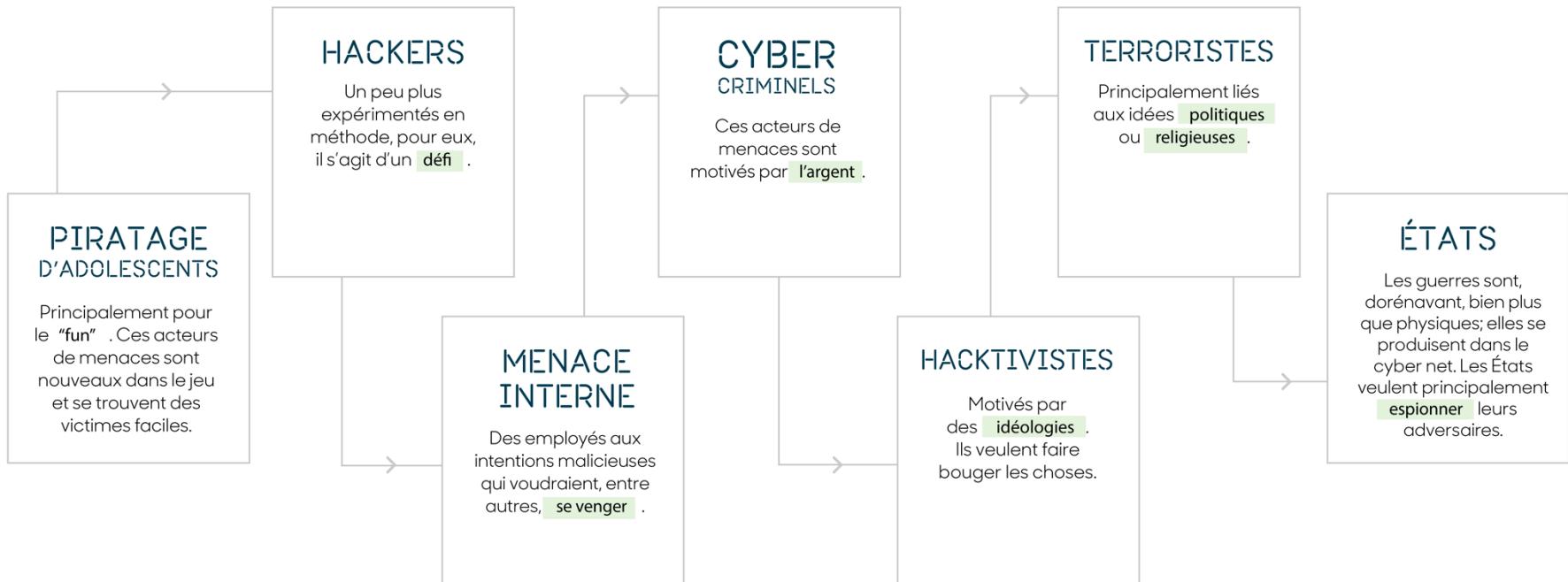
Qui se cachent derrière ces attaques et pourquoi?



+

-

NIVEAU D'EXPOSITION DES PME



-

+

SOPHISTICATION DE L'ATTAQUE



Objectifs de la Trousse Cybereco pour les entreprises

Objectifs de la Trousse



À l'aide de cette trousse nous souhaitons vous sensibiliser, ainsi que vos employés, sur l'importance d'avoir de bonnes pratiques en matière de cybersécurité.

Nous souhaitons également vous guider dans cette démarche et vous donner quelques outils vous permettant d'augmenter votre maturité en cybersécurité.

Thèmes choisis



Plusieurs thèmes seront abordés dans cette trousse dont, entre autres, l'**ingénierie sociale**, les **mots de passe**, la **fraude à la personnalisation** et le **travail en mobilité**.

Des compléments d'information relatifs à d'autres thèmes sont également mis à votre disposition dans les aide-mémoires.





Contenu de la Trousse

Contenu de la Troussse



La présente trousse contient plusieurs éléments décrits ci-dessous :

Un **guide de réunion** pour parler d'un thème de cybersécurité lors de votre prochaine réunion d'équipe

- Vous voulez aborder un de ces thèmes de cybersécurité lors de votre prochaine réunion avec vos employés ? Nous vous avons préparé un guide de réunion avec les bons messages à communiquer. Il s'adapte à une courte réunion de 10mins comme à une plus longue de 30 minutes.

Une **vidéo** de sensibilisation que vous pouvez présenter à vos collaborateurs

- Vous pouvez facilement présenter une vidéo de sensibilisation de courte durée et recensant les bonnes pratiques à adopter pour contrer différents stratagèmes de fraude.

Deux **affiches** que vous pouvez mettre en place dans vos bureaux

- Si vous voulez vous assurer que vos employés n'oublient pas l'importance de rester vigilants, rien de mieux que de placer des affiches dans les endroits stratégiques de vos bureaux.

Un **quiz** qui testera les connaissances de vos employés

- Ce quiz est un bon moyen pour vos employés de tester leurs connaissances et leurs réflexes. Les mises en situation aideront vos employés à mieux réagir lors d'une vraie cyberattaque.

Vous êtes maintenant prêt pour la prochaine étape!



Explorez les grands thèmes de cybersécurité et les outils que nous mettons à votre disposition afin de sensibiliser vos employés.

En collaboration avec

