Boîte à outils des mesures faciles pour les employés et les gestionnaires

Découvrez... *pourquoi est-ce un problème*!

Milieu de travail sécuritaire

 Cartes d'accès à l'immeuble	 Évacuations de l'immeuble		 Risques pour la sécurité personnelle	 Accès aux immeubles / aires de travail

Sauvegarde, stockage, envoi et réception sécuritaires

 Signatures de courriel	 Envoyer des renseignements de nature délicate par courriel	 Envoyer un courriel à des comptes personnels	 Courriel (réfléchissez d'abord)	 Clés USB
 Hameçonnage – cliquer sur des liens	 Hameçonnage – ce qu'il faut considérer	 Arnaques téléphoniques	 Envoi de documents sensibles	 Bureaux bien organisés

Matériel sécuritaire

 Sécuriser physiquement les ordinateurs (au bureau)	 Sécuriser physiquement les ordinateurs (à l'extérieur du bureau)		 Appareils personnels au bureau	 À faire : fin de la journée de travail

Table des matières

Pourquoi est-ce un problème…

…si j'ai prêté ma carte d'identité ou ma carte d'accès à un collègue?

Pourquoi est-ce un problème
• Vous serez tenu responsable à titre de titulaire de la carte d'identité ou de la carte d'accès si un incident survient (p. ex. perte de la carte d'accès, accéder à des zones restreintes).
Scénario
Phil, votre collègue de travail, a oublié sa carte d'identité ou sa carte d'accès. Il sait que vous devez vous rendre à une réunion de deux heures à l'extérieur du bureau et vous demande d'emprunter votre carte pendant votre absence. Que devriez-vous faire?
Mesures possibles (votez pour la bonne réponse)
• Option 1 : Refusez puisque votre carte est pour votre usage seulement. • Option 2 : Prêtez votre carte d'identité ou votre carte d'accès à Phil. • Option 3 : Suggérez à Phil de demander à un autre collègue.
Explication
• L'option 1 est la bonne réponse. • En refusant de prêter votre carte d'identité ou votre carte d'accès, vous respectez les privilèges et les règles d'utilisation associés à la carte qui vous est assignée.
Messages clés à retenir
• Vous ne devez jamais prêter votre carte d'identité ou carte d'accès à qui que ce soit. • Vous devez porter votre carte d'identité ou votre carte d'accès de façon visible, et ce, tous les jours et tout au long de la journée lorsque vous êtes dans les locaux du Ministère. • Si vous avez oublié votre carte d'identité ou votre carte d'accès, veuillez aviser votre gestionnaire ou votre chef d'équipe afin qu'il puisse prendre les dispositions temporaires nécessaires. • Si vous avez perdu votre carte ou si celle-ci a été volée, veuillez aviser immédiatement votre gestionnaire ou votre chef d'équipe et remplir un rapport d'incident de sécurité.
Pour de plus amples renseignements
• Sécurité matérielle

Pourquoi est-ce un problème…

…si je ne me rends pas au lieu de rassemblement désigné par mon équipe lors d'une évacuation?

Pourquoi est-ce un problème
• Votre gestionnaire ou votre chef d'équipe ainsi que vos collègues ne sauront pas si vous avez quitté l'immeuble et ne pourront comptabiliser votre présence. • Vous ne pourrez connaître les renseignements ou les directives à suivre qui seront fournis.
Scénario
Vous présidez une rencontre et soudainement l'alarme sonne indiquant que vous devez sortir. Que devriez-vous faire?
Mesures possibles (votez pour la bonne réponse)
• Option 1 : Quittez l'immeuble et comme c'est pratiquement l'heure du dîner, vous prenez le temps de ramasser votre diner. • Option 2 : Terminez rapidement votre rencontre et vous vous rendez à votre lieu désigné de rassemblement. • Option 3 : Sécurisez vos documents de travail et quittez l'immeuble et vous vous rendez immédiatement à votre lieu de rassemblement.
Explication
• L'option 3 est la bonne réponse. • Vous devez toujours vous rendre immédiatement au lieu de rassemblement désigné pour votre équipe. Ainsi, votre gestionnaire ou votre chef d'équipe ainsi que vos collègues sauront que vous avez quitté l'immeuble en toute sécurité et pourront vous fournir les directives et renseignements pertinents.
Messages clés à retenir
• Assurez-vous de connaître le lieu de rassemblement désigné pour votre équipe. • Lorsque vous entendez l'alarme d'évacuation, quittez l'immeuble de façon calme et ordonnée et rendez-vous directement au lieu de rassemblement désigné pour votre équipe. • Ne pas retarder inutilement la sortie de l'immeuble (p. ex. en envoyant des messages textes, en vous arrêtant pour parler ou en attendant qu'un collègue vous rejoigne). • Assurez-vous de suivre les directives fournies par votre gestionnaire, votre chef d'équipe ou les membres de l'organisme de secours de l'immeuble.
Pour de plus amples renseignements
• Guide des employés sur les situations d'urgence • Trousse d'outils sur les situations d'urgence et l'évacuation des immeubles destinées auxéquipes

Pourquoi est-ce un problème…

…si je ne signale pas un incident impliquant une menace à l'égard de ma sécurité personnelle?

Pourquoi est-ce un problème
• Il est important de souligner tout d'abord que vous êtes important pour nous! Le fait de ne pas signaler immédiatement un incident pourrait compromettre votre bien-être ou celui des autres. • EDSC s'est engagé à veiller à ce que tous les employés soient protégés contre la violence en milieu de travail. Si une situation menaçant votre sécurité personnelle ou la sécurité des autres survient, le Ministère doit être avisé afin d'y donner suite immédiatement et de prendre les mesures nécessaires.
Scénario
À la suite d'un appel téléphonique tendu, un client d'assurance emploi vous a menacé de venir à votre bureau pour vous donner une correction. Que devriez-vous faire?
Mesures possibles (votez pour la bonne réponse)
• Option 1 : Informez votre gestionnaire ou votre chef d'équipe et compléter le rapport d'incident de sécurité. • Option 2 : Ignorez la menace, car vous ne croyez pas que le client y donnera suite. • Option 3 : Indiquez à votre gestionnaire ou à votre chef d'équipe que vous ne vous sentez pas bien et vous vous rendez à votre domicile immédiatement.
Explication
• L'option 1 est la bonne réponse. • Lorsqu'une situation de nature menaçante survient, vous devez le signaler immédiatement à votre gestionnaire ou à votre chef d'équipe et compléter le rapport d'incident de sécurité. Ces procédures ont été mises en place afin d'aider le Ministère à assurer la sécurité de tous les employés.
Messages clés à retenir
• Vous êtes important pour nous! • N'ayez pas peur de signaler des situations qui pourraient représenter un risque pour votre sécurité ou la sécurité des autres. • Votre gestionnaire ou votre chef d'équipe vous répondra et vous donnera le soutien dont vous avez besoin, pour recueillir les faits et de mettre en œuvre les mesures requises. • Le Ministère ne sera pas en mesure de vous aider ni de donner suite à la situation si celle-ci n'est pas signalée. Remarque : Dans le cas d'une menace immédiate, composez le 911 et avisez votre gestionnaire ou votre chef d'équipe.
Pour de plus amples renseignements
• Directive – La sécurité personnelle en milieu de travail • Rapport d'incident de sécurité – ADM3061

Pourquoi est-ce un problème…

…si je tiens la porte ouverte pour quelqu'un derrière moi?

Pourquoi est-ce un problème
• Vous ne savez pas si la personne est là pour des raisons valables ou s'il s'agit d'un voleur ou d'une personne représentant une menace pour votre sécurité personnelle. • Vous pourriez mettre votre sécurité et celle de vos collègues en péril. • Vous pourriez exposer les renseignements et les biens ministériels à des risques de dommages et de vol.
Scénario
En arrivant sur votre étage, vous remarquez quelques personnes se tenant debout près de la porte d'entrée de votre lieu de travail. Que devriez-vous faire?
Mesures possibles (votez pour la bonne réponse)
• Option 1 : Utilisez votre carte d'accès pour entrer à votre lieu de travail et vous vous dirigez vers votre bureau. • Option 2 : Déverrouillez la porte avec votre carte d'accès, puis vous tenez la porte ouverte pour laisser les gens entrer dans votre lieu de travail. • Option 3 : Utilisez votre carte d'accès pour entrer à votre lieu de travail et vous vous assurez que la porte se referme et se verrouille derrière vous.
Explication
• L'option 3 est la bonne réponse. • Le fait d'utiliser votre carte d'accès et de vérifier que la porte est bien verrouillée derrière vous, envoie un message clair indiquant que les autres personnes ne peuvent entrer dans l'immeuble sans leur propre carte d'accès.
Messages clés à retenir
• Tenir la porte ouverte pour d'autres personnes, pour être polis, peut exposer les personnes qui travaillent à l'intérieur d'un immeuble, les renseignements et les biens qui se trouvent sur les lieux à risque. • Toutes les personnes bénéficiant d'un accès autorisé à des immeubles ministériels reçoivent leur propre carte d'accès pour leur permettre d'entrer. • Des processus ont été mis en place pour fournir aux visiteurs l'accès temporaire aux lieux de travail.
Pour de plus amples renseignements
• Vidéo sur le passage en double • Sécurité matérielle

Pourquoi est-ce un problème…

…si je n'utilise pas le bloc de signature normalisé?

Pourquoi est-ce un problème
• Le destinataire supprimera fort probablement votre courriel en pensant qu'il s'agit d'un pourriel ou le signalera comme étant une attaqued'hameçonnage. • Le Secrétariat du Conseil du Trésor (SCT) exige que vous utilisiez un bloc de signature normalisé aux fins d'identification ainsi que pour éviter les doutes concernant la légitimité du courriel. • Un nouveau système de courriel sera bientôt instauré au sein du Ministère pour normaliser toutes les adresses de courriel. Votre bloc de signature sera le seul moyen qu'une personne aura de déterminer pour quel ministère vous travaillez.
Scénario
On vous dit que vos courriels ont été supprimés et non lus car la provenance n'était pas évidente. Que devriez-vous faire?
Mesures possibles (votez pour la bonne réponse)
• Option 1 : Utilisez le bloc de signature officiel conformément aux lignes directrices du Conseil du Trésor. • Option 2 : Créez votre bloc de signature personnalisé qui inclut une pensée du jour. • Option 3 : Indiquez une formule de politesse et votre nom en guise de signature à la fin du courriel.
Explication
• L'option 1 est la bonne réponse. • Vous devez utiliser le bloc de signature officiel du Conseil du Trésor pour vous assurer que vos courriels sont bien identifiés et ne sont pas considérés à tort comme de l'hameçonnage. • La norme du SCT pour les signatures de courriel comprend les éléments suivants (en formatbilingue, toujours) : Nom Titre, Direction générale Ministère / Gouvernement du Canada Courriel / Numéro de téléphone / Numéro de téléimprimeur
Messages clés à retenir
• Pour éviter toute confusion, utilisez un bloc de signature normalisé dans tous vos courriels.
Pour de plus amples renseignements
• Modèle de bloc de signature • Norme sur la gestion du courriel du SCT

Pourquoi est-ce un problème…

…si je transmets par courriel des renseignements de nature délicate?

Pourquoi est-ce un problème
• Il est important de connaître le niveau de confidentialité des renseignements que vous transmettez par courriel. Les renseignements de nature délicate que vous envoyez pourraient être à risque s'ils sont perdus, interceptés ou transmis à la mauvaise personne.
Scénario
Votre collègue dans un autre ministère a demandé un document indiquant une date de naissance et un numéro d'assurance social (NAS). Que dois-je faire?
Mesures possibles (votez pour la bonne réponse)
• Option 1 : Vous chiffrez le document à l'aide d'Entrust puis vous le transmettez par courriel. • Option 2 : Vous insérez le NAS à la ligne objet du courriel afin d'avertir votre collègue. • Option 3 : Vous envoyez le document tel quel.
Explication
• L'option 1 est la bonne réponse. Un courriel indiquant un NAS et un autre renseignement personnel est classé « Protégé B » et doit être chiffré. • La clé est de savoir ce qui constitue un renseignement « Protégé B ». Un courriel qui indique un renseignement personnel tel un NAS n'est pas classé « Protégé B » en soi et, par conséquent, le courriel n'a pas à être chiffré. • Toutefois, il est bon de prendre des mesures préventives et de chiffrer avant l'envoi de documents contenant des renseignements de nature délicate. Par contre, lorsque vous transmettez des renseignements « Protégé B » à l'extérieur du pare-feu ministériel, ceux-ci doivent être chiffrés à l'aide d'Entrust.
Messages clés à retenir
• Réfléchissez à l'information que vous transmettez, à son niveau de confidentialité et veillez à ce qu'elle soit adéquatement protégée. • Vous ne devez indiquer aucun nom, NAS, code d'identification de dossier personnel (CIDP), date de naissance ou toute autre information personnelle dans la ligne objet des courriels. • De plus, vous devez vous assurer que le destinataire est autorisé à consulter les renseignements contenus dans le document (principe d'accès sélectif). • Lorsque vous transmettez un courriel à l'extérieur du système de courriel d'EDSC, nous ne sommes plus en mesure de gérer la sécurité des renseignements transmis dans le courriel. • Le destinataire doit également posséder le logiciel Entrust pour être en mesure d'ouvrir le document.
Pour de plus amples renseignements
• Envoi de renseignements protégés par courriel • Transmettre des renseignements de façon sécuritaire • Comment chiffrer un document (PDF, 187 Ko) • Comment envoyer un courriel chiffré (PDF, 206 Ko) • Gestion de l'information et mesures de protection requises

Pourquoi est-ce un problème…

…si je transmets par courriel des fichiers de travail afin de pouvoir les ouvrir sur mon ordinateur personnel?

Pourquoi est-ce un problème
• Vous compromettez la confidentialité des renseignements. Le courriel pourrait se perdre, être intercepté ou encore être transmis accidentellement à la mauvaise personne. • Vous ne pouvez garantir la sécurité des fichiers pendant leurs transfertsni lorsqu'ils sont stockés dans votre ordinateur personnel.
Scénario
Vous devez préparer un rapport dont le dépôt est prévu demain matin, mais vous ne serez pas en mesure de le terminer au bureau. Vous souhaitez l'envoyer à la maison pour le terminer. Que devriez-vous faire?
Mesures possibles (votez pour la bonne réponse)
• Option 1 : Transmettez le document par courriel pour l'ouvrir sur votre ordinateur à lamaison puisque cette situation ne surviendra qu'une seulefois. • Option 2 : Obtenez l'approbation de votre gestionnaire et empruntez l'équipement ministériel approprié (p. ex. clé USB chiffrée ou ordinateurportatif). • Option 3 : Protégez votre document à l'aide d'un mot de passe puis transmettez-le par courriel afin de l'ouvrir sur votre ordinateur à lamaison.
Explication
• L'option 2 est la bonne réponse. Votre gestionnaire vous aidera à emprunter l'équipement approprié. • La transmission de fichiers de travail vers votre compte de courriel personnel constitue une violation des règles de sécurité. • La protection des documents à l'aide d'un mot de passe ne constitue pas une mesure de sécurité suffisante. Les mots de passe peuvent être facilement décryptés.
Messages clés à retenir
• Si vous devez travailler à la maison, veuillez discuter avec votre gestionnaire. Les appareils appropriés vous seront prêtés (c.-à-d. ordinateur portatif, clé USB chiffrée). • La transmission de documents de travail vers votre ordinateur personnel constitue une violation des règles de sécurité.
Pour de plus amples renseignements
• Apporter du travail à la maison - un diagramme décisionnel • Directive relative à l'utilisation du réseau (voir la section5.9)

Pourquoi est-ce un problème…

…si j'utilise la fonction « Répondre à tous » dans un courriel sans vérifier la liste des destinataires?

Pourquoi est-ce un problème
• Vous pourriez divulguer des renseignements de nature délicate à des personnes qui ne devraient pas obtenir ces renseignements. • Vous pourriez créer de la confusion chez certains destinataires qui ne comprendront pas pourquoi ils reçoivent votre courriel. • Vous pourriez provoquer une panne du réseau électronique du Ministère.
Scénario
Vous recevez un courriel provenant d'une grande liste de distribution et vous devez fournir une réponse. En premier lieu, que devriez-vous faire?
Mesures possibles (votez pour la bonne réponse)
• Option 1 : Envoyez le message en utilisant la Cci (copie conforme invisible) pour éviter que tous reçoivent le courriel. • Option 2 : Répondre à tous puisqu'il doit y avoir une raison si le courriel a été envoyé à tous. • Option 3 : Réfléchissez à la raison pour laquelle vous faites part de la liste de distribution et décidez si l'utilisation de la fonction « Répondre à tous » est le bon choix.
Explication
• L'option 3 est la bonne réponse. • Le champ Cci empêche les destinataires de répondre à tous mais prenez le temps d'examiner s'ils doivent tous connaître votre réponse. Le champ répondre à tous ne doit être utilisé que si tous les destinataires doivent connaître la réponse et pouvoir ainsi répondre à tous.
Messages clés à retenir
• Vérifiez la liste des destinataires avant de répondre à un courriel. • La fonction « Répondre à tous » doit être utilisée avec précaution, quelle que soit la liste de distribution. • Assurez-vous de connaître vos obligations en ce qui a trait à la Directive sur l'utilisation du réseau.
Pour de plus amples renseignements
• Directive sur l'utilisation du réseau d'EDSC

Pourquoi est-ce un problème…

…si j'utilise une clé USB personnelle à des fins professionnelles?

Pourquoi est-ce un problème
• Si vous la perdez ou l'égarez, vous aurez alors également perdu ou égaré l'information (du Ministère) qui s'y trouve. • La politique d'EDSC stipule que dans le cadre de leur travail, tous les employés doivent utiliser un dispositif fourni par le Ministère.
Scénario
Vous devez apporter des fichiers en version électronique à une réunion demain. Vous songez à vous procurer une clé USB du Ministère, mais vous réalisez rapidement que vous ne disposez pas suffisamment de temps pour obtenir l'approbation requise. Que devriez-vous faire?
Mesures possibles (votez pour la bonne réponse)
• Option 1 : Utilisez une clé USB personnelle avec laquelle vous n'avez jamais eu de problème parle passé. • Option 2 : Allez acheter une nouvelle clé USB, vous serez ainsi certain qu'elle est sécuritaire. • Option 3 : Envoyez les fichiers par courriel au président de la réunion ou stockez-les sur un ordinateur portatif du Ministère pour les apporter avec vous.
Explication
• L'option 3 est la bonne réponse. • Envoyer les fichiers par courriel est la méthode la plus simple, à condition que l'information n'ait pas une cote de sécurité supérieure à « Protégé B ». Si vous avez un ordinateur portatif du Ministère à votre disposition, vous pouvez y stocker vos fichiers. • Même si vous n'avez jamais eu de problème avec une clé USB personnelle par le passé, cela ne signifie pas qu'il est sécuritaire de l'utiliser pour y stocker des renseignements liés au travail. • Les clés USB neuves achetées en magasin peuvent être altérées au cours de la production. Ainsi, même si vous croyez qu'elles sont sécuritaires, elles ne le sont peut-être pas. De plus, vous pouvez également perdre ou égarer ces clés.
Messages clés à retenir
• Vous devez toujours utiliser des dispositifs (ordinateurs portatifs, clés USB) fournis par le Ministère pour transporter des renseignements ministériels. • Seuls les dispositifs USB fournis par le Ministère peuvent être connectés au réseau.
Pour de plus amples renseignements
• Dispositifs de stockage portatifs • Dispositifs portatifs approuvés

Pourquoi est-ce un problème…

…si je clique sur ce lien dans un courriel suspect?

Pourquoi est-ce un problème
• Vous pourriez installer un virus qui peut mettre votre ordinateur et l'information qu'il contient à risque. Cela constitue un risque pour le Ministère. • Vous pourriez lancer un logiciel espion qui permettrait à un cybercriminel de voler votre mot de passe. Ce mot de passe pourrait être utilisé pour avoir accès à d'autres renseignements sur le réseau électronique d'EDSC. • Cela pourrait mener à : la perte d'information, le vol d'identité, des intrusions sur le réseau, la perte de confiance des clients ou un gain financier pour le cybercriminel.
Scénario
À 4 h 48 vous recevez un courriel indiquant que votre ordinateur a peut-être un virus. On vous demande de cliquer sur le lien et d'entrer votre nom d'utilisateur et votre mot de passe pour faire un balayage informatique dans le but de détecter les virus. Que devriez-vous faire?
Mesures possibles (votez pour la bonne réponse)
• Option 1 : Supprimez le courriel • Option 2 : Cliquez sur le lien et entrez les renseignements • Option 3 : Rapportez le message en ligne à l'InfoService national (à l'aide de l'icône représentant un hameçon)
Explication
• L'option 3 est la bonne réponse. • Si un message électronique vous semble suspect, spécialement si l'on vous demande des renseignements personnels (p. ex. mot de passe, nom d'utilisateur), vous devez le rapporter à l'InfoService national.
Messages clés à retenir
• N'ouvrez les courriels de sources inconnues qu'avec extrême prudence. • S'ils vous semblent suspects, ne prenez aucun risque. Ne répondez pas, ne cliquez sur aucun lien et n'ouvrez aucune pièce jointe. Signaler immédiatement de tels courriels en ligne à l'InfoService national. Puis, supprimez le courriel.
Pour de plus amples renseignements
• Vidéo : HALTE à l'hameçonnage

Pourquoi est-ce un problème…

…si je ne sais pas à quoi ressemble un courriel d'hameçonnage?

Pourquoi est-ce un problème
• Vous exposez le réseau électronique de notre ministère à des risques si vous vous faites piéger et que vous cliquez sur une pièce jointe ou un lien infecté. Par inadvertance, vous pourriez télécharger des logiciels espions ou malveillants.
Scénario
Vous recevez un courriel ayant pour objet « Affaire urgente » et le courriel contient un fichier PDF. Ce dernier pourrait traiter du nouveau contrat auquel vous travaillez, mais vous savez que ce fichier pourrait être un leurre. Quels sont les indices que vous devez rechercher pour déterminer s'il s'agit d'un courriel d'hameçonnage?
Mesures possibles (votez pour la bonne réponse)
• Option 1 : Vérifier l'horodatage, le bloc de signature, les erreurs d'orthographe et de grammaire, les salutations génériques. • Option 2 : Vérifier s'il y a des petits changements aux noms de domaine du courriel. • Option 3 : Survoler le lien avec le curseur pour que s'affiche l'URL véritable.
Explication
• Les options 1, 2 et 3 sont toutes valables! Ce ne sont que quelques-uns des indices qui peuvent vous aider à déterminer s'il s'agit d'un courriel d'hameçonnage. • Vous devez examiner tous ces éléments ensemble. Si quelque chose cloche, signalez le courriel en ligne à l'aide de l'icône représentant un hameçon sur la page de l'InfoService national.
Messages clés à retenir
• Les courriels d'hameçonnage sont l'une des méthodes les plus couramment utilisées par les cybercriminels pour voler des renseignements, c'est pourquoi vous devez savoir comment reconnaître ce type de courriel. • Ouvrez les courriels provenant d'expéditeurs inconnus avec une extrême prudence. Utilisez HALTE, qui vous permettront de déterminer s'il s'agit d'un courriel digne de confiance. • Si le courriel vous semble suspect, il l'est probablement! N'y répondez pas, ne cliquez sur aucun lien et n'ouvrez pas les pièces qui y sont jointes. Signaler immédiatement de tels courriels en ligne à l'InfoService national, puis supprimez le courriel suspect. • Si vous croyez qu'il pourrait s'agir d'un courriel authentique, mais que vous n'en êtes pas certain et que vous ne voulez pas le supprimer prématurément, vérifier l'adresse courriel ou le numéro de téléphone de l'expéditeur au moyen d'une autre méthode (p. ex. les Services d'annuaires gouvernementaux électroniques, répertoire Outlook). Ensuite, appelez l'expéditeur ou envoyez-lui un nouveau courriel afin de lui demander si le courriel que vous avez reçu est authentique.
Pour de plus amples renseignements
• Halte à l'hameçonnage • Pourriels et courriels d'hameçonnage

Pourquoi est-ce un problème…

…si je ne reconnais pas les indices d'une tentative d'hameçonnage vocal?

Pourquoi est-ce un problème
• Il est probable que vous soyez victime d'une attaque d'hameçonnage vocal et que vous donniez aux cybercriminels l'information ou les moyens nécessaires pour obtenir l'accès à notre réseau électronique, ce qui constitue un risque pour l'information des citoyens canadiens.
Scénario
Vous recevez un appel téléphonique d'un agent de l'équipe de service informatique qui affirme que votre ordinateur est infecté par un virus. L'agent veut savoir quel type de logiciel anti-virus est installé sur votre ordinateur et il vous demande l'accès à distance immédiatement pour qu'il puisse nettoyer votre ordinateur et ce, avant que le virus n'infecte l'ordinateur de tous les autres employés. Quels sont les indices vous permettant de croire qu'il s'agit d'une tentative d'hameçonnage vocal?
Mesures possibles (votez pour la bonne réponse)
• Option 1 : L'agent vous demande de lui donner l'accès à distance à votre ordinateur pour qu'il puisse le nettoyer. • Option 2 : L'agent vous demande quel logiciel anti-virus est installé sur votre ordinateur. • Option 3 : La personne utilise la peur pour vous inciter à accepter son aide.
Explication
• Toutes les options présentées sont des indices d'une tentative d'hameçonnage vocal. • Les employés de l'InfoService national du Ministère (GI-TI) ne vous demanderont jamais quels logiciels sont installés sur votre ordinateur car ils le savent déjà. • L'InfoService national n'a pas besoin de l'accès à distance pour supprimer un virus de votre ordinateur.
Messages clés à retenir
• Ne répondez pas à des questions douteuses concernant le système informatique du Ministère. • Ne donnez pas l'accès à distance à votre ordinateur à moins que vous ne soyez certain qu'il s'agit d'une demande légitime (par exemple, les demandes légitimes sont présentées par l'InfoService national ou un groupe de résolution à la suite d'une demande de service que vous avez déposée). • En cas de doute, raccrochez et parlez-en à votre chef d'équipe/gestionnaire le plus tôt possible. Votre chef d'équipe ou gestionnaire doit ensuite communiquer avec le Bureau régional de la sécurité pour signaler l'incident. • Ne vous fiez pas à l'identification de l'appelant de votre téléphone car les numéros de téléphone peuvent être falsifiés.
Pour de plus amples renseignements
• Hameçonnage vocal

Pourquoi est-ce un problème…

…si j'envoie des documents de nature délicate par courrier de la même façon que je procède pour envoyer une carte de souhaits?

Pourquoi est-ce un problème
• L'enveloppe pourrait être ouverte par inadvertance ou par quelqu'un qui ne doit pas voir son contenu. • Cette personne aurait désormais en sa possession des renseignements de nature délicate, notamment des renseignements qui pourraient être personnels et qu'elle n'est pas autorisée à avoir. • Cette situation pourrait entraîner de la fraude, un vol d'identité ou une mauvaise utilisation des renseignements.
Scénario
Au cours d'une investigation de dossier, un agent de l'Agence du revenu Canada (ARC) vous demande de lui fournir une copie d'un dossier client qui contient des documents classé « Protégé B ». Le télécopieur sécurisé de votre bureau a été envoyé en réparation. Que devriez-vous faire?
Mesures possibles (votez pour la bonne réponse)
• Option 1 : Attendez que le télécopieur sécurisé soit réparé. • Option 2 : Insérez le dossier du client dans une enveloppe double et l'envoyer par courrier à l'ARC. • Option 3 : Envoyez les renseignements à l'ARC à l'aide d'un télécopieur régulier.
Explication
• L'option 2 est la bonne réponse. • Lorsque vous utilisez une enveloppe double, l'enveloppe extérieure ne fait pas mention des renseignements de nature délicate qu'elle contient ou n'attire pas l'attention sur ceux-ci. • Si l'enveloppe est ouverte par inadvertance à l'ARC, une autre enveloppe à l'intérieur indique à la personne que le contenu est de nature délicate et qu'il doit être remis à un destinataire précis.
Messages clés à retenir
• Toujours adopter les mesures de protection et les lignes directrices adéquates pour envoyer des renseignements de nature délicate par courrier. • Lorsque vous utilisez des enveloppes doubles – indiquez sur l'enveloppe intérieure le niveau de classification de sécurité approprié (p. ex. « Protégé B »). Cela permet d'aviser le destinataire du niveau de confidentialité des renseignements et favorise la mise en application des mesures de protection requises pour la distribution.
Pour de plus amples renseignements
• Guide de classification de l'information • Gestion de l'information et mesures de protection requises

Pourquoi est-ce un problème…

…si je laisse des dossiers sur mon bureau ou ouverts à mon ordinateur?

Pourquoi est-ce un problème
• Toute personne qui passe par votre bureau pourrait voir des renseignements qu'elle ne devrait pas voir. • Ces renseignements pourraient être copiés, modifiés ou pris sur votre bureau ou votre ordinateur. • Vous risquez de devoir expliquer pourquoi les renseignements dont vous aviez la garde ont été perdus, copiés ou modifiés si un incident ou une enquête de sécurité avait lieu.
Scénario
Vous travaillez à votre bureau sur deux dossiers papier de clients qui sont « Protégé B ». Votre gestionnaire vous demande de l'accompagner immédiatement à une rencontre avec le directeur. Que devriez-vous faire?
Mesures possibles (votez pour la bonne réponse)
• Option 1 : Retournez vos documents face contre le bureau et quittez immédiatement pour la rencontre. • Option 2 : Rangez les deux dossiers dans un classeur verrouillé et vous verrouillez également votre ordinateur. • Option 3 : Laissez les dossiers ouverts sur votre bureau comme vous travaillez dans une zone à accès restreint, vous êtes sûr qu'il n'y aura pas de problème.
Explication
• L'option 2 est la bonne réponse. • En rangeant les dossiers dans un classeur verrouillé, vous protégez les renseignements des clients contre tout accès non autorisé. • Verrouiller votre ordinateur empêche tout accès non autorisé ou toute modification des fichiers électroniques (y compris les courriels).
Messages clés à retenir
• Vous ne voulez pas être responsable de la perte de renseignements ou que des renseignements se retrouvent dans les mains de personnes malveillantes, surtout lorsqu'il s'agit de renseignements personnels ou de nature délicate. • Vous devez toujours protéger les renseignements (sur papier et en format électronique) dont vous avez la garde lorsque vous vous absentez de votre bureau. • Les renseignements non sécurisés sont vulnérables.
Pour de plus amples renseignements
• Lignes directrices pour un bureau bien organisé • Guide de classification de l'information • Gestion de l'information et mesures de protection requises

Pourquoi est-ce un problème…

…si je ne protège pas mes dispositifs électroniques lorsque je ne suis pas à mon bureau?

Pourquoi est-ce un problème
• Quelqu'un pourrait voler ou endommager vos dispositifs. • Quelqu'un pourrait voler ou falsifier les renseignements qui se trouvent sur vos dispositifs (ou sur le réseau électronique d'EDSC).
Scénario
À votre retour après une réunion, vous constatez que vous avez laissé votre appareil BlackBerry sur votre bureau. Que devriez-vous faire avant de quitter votre bureau?
Mesures possibles (votez pour la bonne réponse)
• Option 1 : Rien, vous avez confiance en vos collègues des bureaux voisins. • Option 2 : Placez votre appareil BlackBerry dans une armoire verrouillée ou apportez-le avec vous. • Option 3 : Mettez votre appareil BlackBerry hors tension.
Explication
• L'option 2 est la bonne réponse – il est primordial de protéger vos dispositifs pour assurer la sécurité de l'appareil ainsi que l'information qui s'y trouve. • Vos collègues ne sont pas les seules personnes qui ont accès à votre bureau – les clients, les visiteurs et le personnel de l'immeuble doivent aussi être pris en considération. • La mise hors tension de vos dispositifs ne les protège pas du vol.
Messages clés à retenir
• Prenez le temps de mettre vos dispositifs, même si vous ne vous absentez que pour une minute. • Protégez vos dispositifs et protégez les renseignements qu'ils contiennent.
Pour de plus amples renseignements
• Sécurité de l'espace de travail et du bureau

Pourquoi est-ce un problème…

…si j'utilise mon ordinateur personnel pour travailler à l'extérieur du bureau?

Pourquoi est-ce un problème
• Votre ordinateur personnel n'est pas protégé sur le plan de la sécurité de la même façon que le réseau électronique d'EDSC est protégé. • Si vous perdez votre ordinateur, l'information contenu (qui appartient au Ministère et aux Canadiens) est également perdue. • Si d'autres personnes à votre domicile ont accès à votre ordinateur, ils ont accès à des renseignements auxquels ils n'ont pas droit. • En aucun cas, vous ne devriez envoyer par courriel des renseignements concernant le travail (ou vice versa) puisque cela crée un risque encore plus grand pour la sécurité.
Scénario
Vous avez prévu travailler à la maison demain. En route pour la maison, vous réalisez que vous avez oublié votre ordinateur portatif de travail. Que devriez-vous faire?
Mesures possibles (votez pour la bonne réponse)
• Option 1 : Envoyez un courriel à un collègue pour lui demander de vous envoyer les fichiers dont vous avez besoin à votre compte personnel de courriel. • Option 2 : Retournez au bureau pour aller chercher votre ordinateur portatif du travail. • Option 3 : Téléphonez à votre gestionnaire et demandez-lui la permission d'utiliser votre ordinateur personnel.
Explication
• L'option 2 est la bonne réponse même si celle-ci nécessite un déplacement supplémentaire au travail. • Votre ordinateur personnel n'est pas un appareil autorisé par le Ministère et c'est pourquoi il ne devrait pas être utilisé pour traiter des renseignements concernant le travail. • Votre gestionnaire ne devrait pas vous donner la permission d'utiliser votre ordinateur personnel pour votre travail. • L'exception serait que vous avez été autorisé à utiliser AppGate pour l'accès au bureau à distance, dans ce cas, vous pouvez donc utiliser votre ordinateur personnel à des fins de travail
Messages clés à retenir
• Vous avez la responsabilité de protéger l'information, peu importe si vous travaillez sur place dans un bureau ou à l'extérieur du bureau. • Le travail que vous effectuez à l'extérieur du bureau doit soit être effectué sur un appareil autorisé par le Ministère en utilisant le réseau privé virtuel (RPV) ou sur votre ordinateur personnel en utilisant AppGate.
Pour de plus amples renseignements
• Sécurité des ordinateurs personnels • Accès RPV et à distance

Pourquoi est-ce un problème…

…si je branche mon téléphone cellulaire personnel sur mon ordinateur de travail?

Pourquoi est-ce un problème
• Votre téléphone cellulaire personnel (ou iPod, ou tablette, ou tout autre dispositif personnel) pourrait être infecté par un logiciel malveillant ou un virus. Lorsque vous branchez ce dispositif, vous faites une connexion sur le réseau électronique d'EDSC et vous pourriez peut-être glisser le logiciel malveillant ou le virus sur notre réseau.
Scénario
Vous attendez un appel personnel et votre pile est pratiquement déchargée. Que devriez-vous faire ?
Mesures possibles (votez pour la bonne réponse)
• Option 1 : Rechargez votre téléphone en le branchant sur votre ordinateur • Option 2 : Rechargez votre téléphone à l'aide d'une prise de courant • Option 3 : Vous ne pouvez pas recharger votre téléphone au travail
Explication
• L'option 2 est la bonne réponse. Pour recharger vos appareils personnels, vous devez utiliser une prise électrique. • Cela vaut pour tous vos appareils personnels (p. ex. lecteurs de musique, appareils photographiques numériques, tablettes, lecteurs électroniques), et non seulement les téléphones cellulaires.
Messages clés à retenir
• Seuls les appareils autorisés peuvent être branchés sur le réseau, car ceux-ci disposent des caractéristiques de sécurité pour protéger les renseignements ministériels. • Il est interdit de brancher vos appareils personnels sur votre poste de travail, sur votre portable ou sur le réseau. • Les ordinateurs ministériels sont balayés informatiquement afin de veiller à ce qu'aucun dispositif USB non autorisé ne soit branché.
Pour de plus amples renseignements
• Supports portatifs approuvés • Directive sur les dispositifs de stockage portatifs

Pourquoi est-ce un problème…

…si je laisse mon ordinateur en marche toute la nuit OU si je l'éteins à la fin de la journée?

Pourquoi est-ce un problème
• Des mises à jour logicielles et d'importants correctifs de sécurité sont installés durant la nuit pendant que vous dormez. • Ces transferts n'auront pas lieu si l'équipement est hors tension ou identifié comme « absent ». • Les mises à jour logicielles permettent aux employés de disposer de la meilleure technologie que puisse offrir EDSC. • Les correctifs de sécurité incluent des mises à jour d'antivirus et des balayages afin de veiller à la sécurité du réseau électronique d'EDSC ainsi qu'à toute l'information qu'il contient.
Scénario
Vous vous préparez à partir en vacances pour trois semaines. Vous désirez agir de la façon la plus écologique possible en économisant l'énergie, donc vous songez à mettre votre ordinateur hors tension. Que devriez-vous faire ?
Mesures possibles (votez pour la bonne réponse)
• Option 1 : Verrouillez votre ordinateur (Ctrl-Alt-Del-Enter) • Option 2 : Redémarrez votre ordinateur (Démarrer-Arrêter-Redémarrer-Ok) • Option 3 : Éteignez l'ordinateur (Démarrer-Arrêter-Ok)
Explication
• L'option 2 est la bonne réponse. • Si vous vous souciez de l'environnement et du gaspillage d'énergie, sachez que certaines technologies sont examinées afin que vous puissiez éventuellement éteindre votre ordinateur à votre départ pour les vacances.
Messages clés à retenir
• Vous devez suivre la procédure appropriée, c'est-à-dire « Démarrer-Arrêter-Redémarrer-Ok» à la fin de la journée. • Même les vendredis et même la dernière journée avant les vacances! • Le fait de ne pas permettre les mises à jour des différents logicielles, des programmes antivirus et des correctifs de sécurité rends votre ordinateur plus vulnérable aux attaques. • Si vous travaillez à l'extérieur du bureau, ne mettez pas votre ordinateur hors tension et ne le redémarrez pas. Vous devez seulement fermer votre session afin de garder votre connexion au réseau active pour permettre l'installation des correctifs et des mises à jour de logiciels.
Pour de plus amples renseignements
• Sécurité sur iService