CANADIAN CENTRE FOR CYBER SECURITY

IDENTIFY AND HANDLE MALICIOUS MESSAGES

All members of a campaign team should know how to identify malicious messages and how to handle them.

Verify that you really know the sender and, if possible, that the tone of the message is consistent with the sender.

Verify that the sender's address is valid. Sometimes threat actors will use addresses that look legitimate, but are altered in very slight ways.

Look for misspelled words in the body of the message. This is a trick used to bypass spam filters.

Look for unusual phrasing in the message, which may suggest that the author isn't legitimate.

Look for an offer that is too good to be true.

Pay attention to a request, which may include a threat, for sensitive information (e.g. personal or financial information).

Ensure the content of the message is relevant to your campaign work if the message is sent to your campaign email address.

Check that included links or attachments are relevant to the content of the message

Never click on links included in malicious or suspicious messages, even if they offer to remove you from a distribution list. If someone sends you a link (e.g a news release) browse to the page or search for it online instead.

Never open attachments included in malicious messages. Malware often hides in attachments.

If you must open an attachment, open it on a computer that is not connected to the campaign IT infrastructure.

Do not reply to suspicious messages or spam messages. Doing so will only confirm that your address is valid, resulting in more spam.

Do not provide any confidential information (e.g user name or password), even if the emails appear legitimate. If the email appears real, contact the sender another way (e.g. call them) to verify the request before providing information.

Do not forward suspicious messages to other people. If you need to show it to someone, ask the person to view it on your screen or print it out.

Delete spam messages or move them to a junk folder. If you're unsure whether it's spam or you don't know what to do with the message, talk to your campaign team lead.

HOW TO HANDLE POTENTIALLY CRIMINAL MESSAGES OR CYBERCRIME

The Royal Canadian Mounted Police (RCMP) generally interprets cybercrime to be any crime where the Internet and information technologies (such as computers, tablets, personal digital assistants, or mobile devices), have a substantial role in the commission of a criminal offence. It includes technically-advanced crimes that exploit vulnerabilities found in digital technologies. It also includes more traditional crimes that take on new shapes in cyberspace.

If you receive an offensive, abusive, or potentially criminal message, whether it seems to be spam, phishing or something else, or if you think criminals are asking you for confidential information, inform your local police and the RCMP. Save the message, as authorities may ask you to provide a copy to help with any subsequent investigations. Do not send the message to others.

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

REPÉRER LES MESSAGES MALVEILLANTS ET SAVOIR QUOI EN FAIRE

Tous les membres de l'équipe de campagne devraient pouvoir repérer des messages malveillants et savoir quoi en faire lorsqu'ils en reçoivent.

Assurez-vous de reconnaître l'expéditeur et, si possible, de confirmer que le ton employé dans le message correspond à celui que cet expéditeur utiliserait normalement.

Validez l'adresse de l'expéditeur. Les auteurs de menaces utilisent parfois des adresses de courriel qui ressemblent à des adresses de courriel d'entreprises légitimes, mais les modifient que très légèrement.

Vérifiez si le corps du message contient des fautes d'orthographe. C'est un truc qui permet de contourner les filtres de pourriel.

Vérifiez si le message contient des formulations inhabituelles, ce qui pourrait mettre en doute la légitimité de son auteur.

Méfiez-vous des offres qui sont trop belles pour être vraies.

Soyez aux aguets des menaces et des demandes d'information sensible (p. ex., information personnelle ou financière).

Si le message est envoyé à une adresse liée à la campagne, veillez à ce que le contenu du message ait trait aux activités de la campagne.

Veillez à ce que les hyperliens et les pièces jointes correspondent au contenu du message.

Ne cliquez jamais sur un lien compris dans un message malveillant ou suspect, même si on vous offre de supprimer votre adresse d'une liste de distribution. Si vous recevez un lien (p. ex., vers un communiqué), entrez l'adresse vous-même ou faites une recherche sur le navigateur Web.

N'ouvrez jamais de pièces jointes contenues dans des messages malveillants. Elles contiennent souvent des maliciels.

Si vous devez ouvrir une pièce jointe, servez-vous d'un ordinateur qui n'est pas branché à l'infrastructure TI de la campagne.

Ne répondez pas aux messages suspects ou aux pourriels. Cela ne fera que confirmer la validité de votre adresse de courriel et aura pour effet de multiplier les pourriels.

Ne fournissez jamais de l'information confidentielle (p. ex., nom d'utilisateur et mot de passe), même si le message semble légitime. Lorsque le message donne l'impression d'être légitime, communiquez avec l'expéditeur par un autre moyen (p. ex., par téléphone) avant de fournir toute information, ce qui a pour but de vérifier la légitimité de la demande.

Ne réacheminez jamais un message suspect à un autre destinataire. Si vous souhaitez le montrer à quelqu'un, demandez à la personne de venir le voir à l'écran ou montrez-lui une copie papier.

Supprimez les pourriels ou déplacez-les dans un dossier de courrier indésirable. Si vous avez des doutes ou ne savez pas quoi faire avec le message, adressez-vous au responsable de l'équipe.

QUE FAIRE AVEC DES MESSAGES DE NATURE CRIMINELLE OU EN CAS DE CYBERCRIME?

La Gendarmerie royale du Canada (GRC) considère généralement que la cybercriminalité concerne tout délit commis principalement au moyen des technologies de l'information et de l'internet, comme un ordinateur, une tablette, un assistant numérique personnel ou un dispositif mobile. Cette définition comprend les crimes commis au moyen de techniques plus sophistiquées pour exploiter les vulnérabilités dans les technologies numériques ainsi que les crimes plus traditionnels qui prennent de nouvelles formes dans le cyberespace.

Si vous recevez un message outrancier ou offensant ou encore un message de nature criminelle (qu'il s'agisse d'un pourriel, d'un courriel d'hameçonnage, ou autres), ou si vous estimez que des criminels vous demandent de divulguer des renseignements personnels, informez-en la police locale ou la GRC. Conservez le message suspect, car les autorités pourraient vous demander d'en produire une copie aux fins d'enquête. Ne réacheminez jamais un message suspect à d'autres destinataires.