Bonnes pratiques en Cybersécurité

Document réalisé par Culture Saguenay–Lac-Saint-Jean

PHISHING : RECONNAÎTRE ET ÉVITER LES COURRIELS FRAUDULEUX

QU'EST-CE QUE LE PHISHING ?

Le phishing (ou hameçonnage) est une technique utilisée par des cybercriminels pour tromper leurs victimes et les pousser à :

1. Divulguer des informations sensibles (mots de passe, numéros de cartes bancaires, identifiants, etc...)
2. Cliquer sur un lien piégé menant à un faux site
3. Télécharger une pièce jointe infectée

TYPES DE PHISHING COURANTS

Type	Cible	Exemple
Spear phishing	Individu spécifique	E-mail personnalisé avec infos réelles
Whaling	Dirigeants	Fausse facture ou document juridique
Clone phishing	Utilisateurs réguliers	Copie d'un e-mail légitime modifié
Pharming	Grand public	Redirection vers faux site bancaire

COMMENT RECONNAÎTRE UN COURRIEL FRAUDULEUX ?

SIGNES COURANTS À SURVEILLER :

Expéditeur suspect

- **Adresse étrange :** ne correspond pas à l'organisation prétendue
- **Imitation d'une organisation connue :** fautes dans le nom de domaine (@amazom.com au lieu de @amazon.com)
- **Adresses génériques :** (@gmail.com, @hotmail.com) pour des entreprises

Liens douteux

- URLs raccourcies (bit.ly, tinyurl.com)
- **Ils ne correspondent pas à l'adresse officielle** (vérifiez en passant la souris dessus)
- Liens ne correspondant pas au texte affiché
- Boutons d'action suspects

Ton urgent ou menaçant

- Votre compte sera bloqué"
- "Action immédiate requise"
- Menaces de fermeture de compte
- Offres trop belles pour être vraies

Fautes d'orthographe/grammaire

- **Courriels mal rédigés**
- Mise en forme approximative
- Formules de politesse génériques
- Logos de mauvaise qualité

Pièces jointes inattendues

- Fichiers **.zip, .exe**, ou documents suspects
- Pièces jointes non sollicitées
- Extensions dangereuses (**.scr, .bat**)

BONNES PRATIQUES POUR ÉVITER LE PIÈGE

✅ **Toujours vérifier l'expéditeur** avant de cliquer

✅ **Ne jamais cliquer directement sur les liens** : tapez l'adresse officielle dans votre navigateur

✅ **Ne jamais fournir vos informations sensibles par courriel**

✅ Utiliser une authentification multifactorielle (**MFA**)

✅ **Mettre à jour régulièrement** vos logiciels et antivirus

✅ **Signaler immédiatement** tout courriel suspect à l'équipe TI ou cybersécurité

Mesures techniques complémentaires

- Configurer les **filtres anti-spam**
- Activer l'**authentification à deux facteurs** sur tous les comptes
- Utiliser un **gestionnaire de mots de passe**.

En cas de réception de courriel suspect

- **Signaler** le message comme spam/phishing
- **Supprimer** le message
- **Informer** ses collègues

QUE FAIRE SI VOUS AVEZ CLIQUÉ PAR ERREUR

Réagissez rapidement !

- **Ne fournissez aucune donnée personnelle**
- **Déconnectez-vous immédiatement** de l'appareil si possible
- **Changez vos mots de passe** depuis un autre appareil sûr
- **Avertissez** votre service informatique pour analyse
- **Surveillez** vos comptes bancaires et courriels pour détecter toute activité suspecte

Si vous avez fourni des informations

- **Signaler** le message comme spam/phishing
- **Supprimer** le message
- **Informer** ses collègues

RAPPEL ET INFOS UTILES

Rappels clés

- UN COURRIEL PEUT **SEMBLER LÉGITIME,** MAIS SI UN **DÉTAIL PARAÎT ÉTRANGE**, IL VAUT MIEUX **NE PAS CLIQUER**.
- Le **réflexe sécurité** = Prudence + Vérification + Signalement
- **Astuce** : Créez un dossier « Courriels suspects » pour aider l'équipe TI à mieux analyser les tentatives d'hameçonnage

Méthodes de verification rapide

- **Survoler les liens sans cliquer** pour voir la vraie destination
- **Contacter directement l'organisation par téléphone**
- Se **connecter** au site officiel par un autre moyen
- **Consulter** un collègue ou le service IT en cas de doute.

RESSOURCES UTILES

- **VÉRIFICATEUR DE LIENS** : ISIT PHISHING, VIRUSTOTAL, URLVOID, SUCURI SITECHECK, PHISHTANK
- **SIGNALEMENT** : AUTORITÉS LOCALES
- **OUTILS** : GESTIONNAIRES DE MOTS DE PASSE, AUTHENTIFICATION 2FA