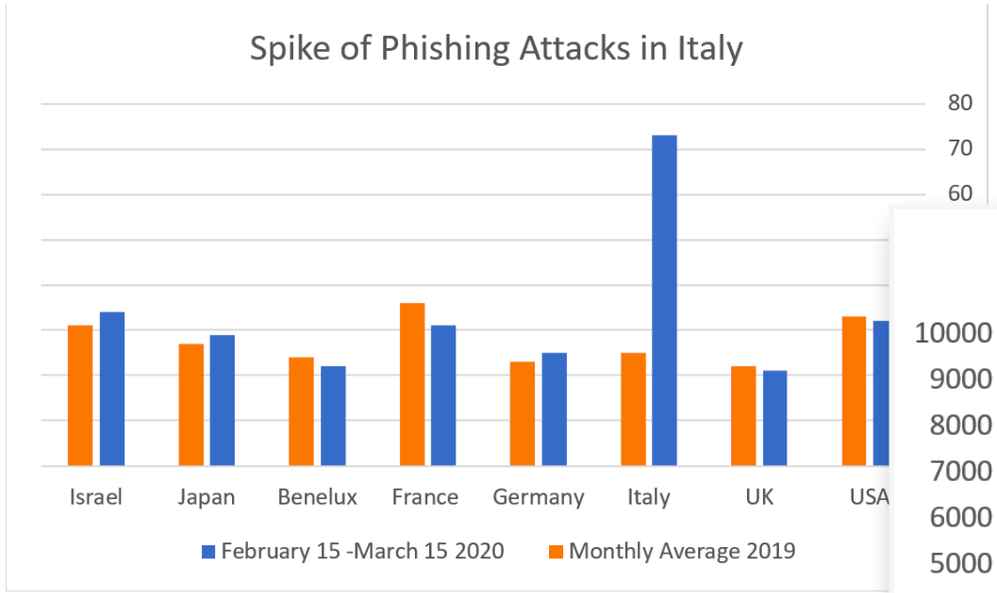
CYBERRISQUES

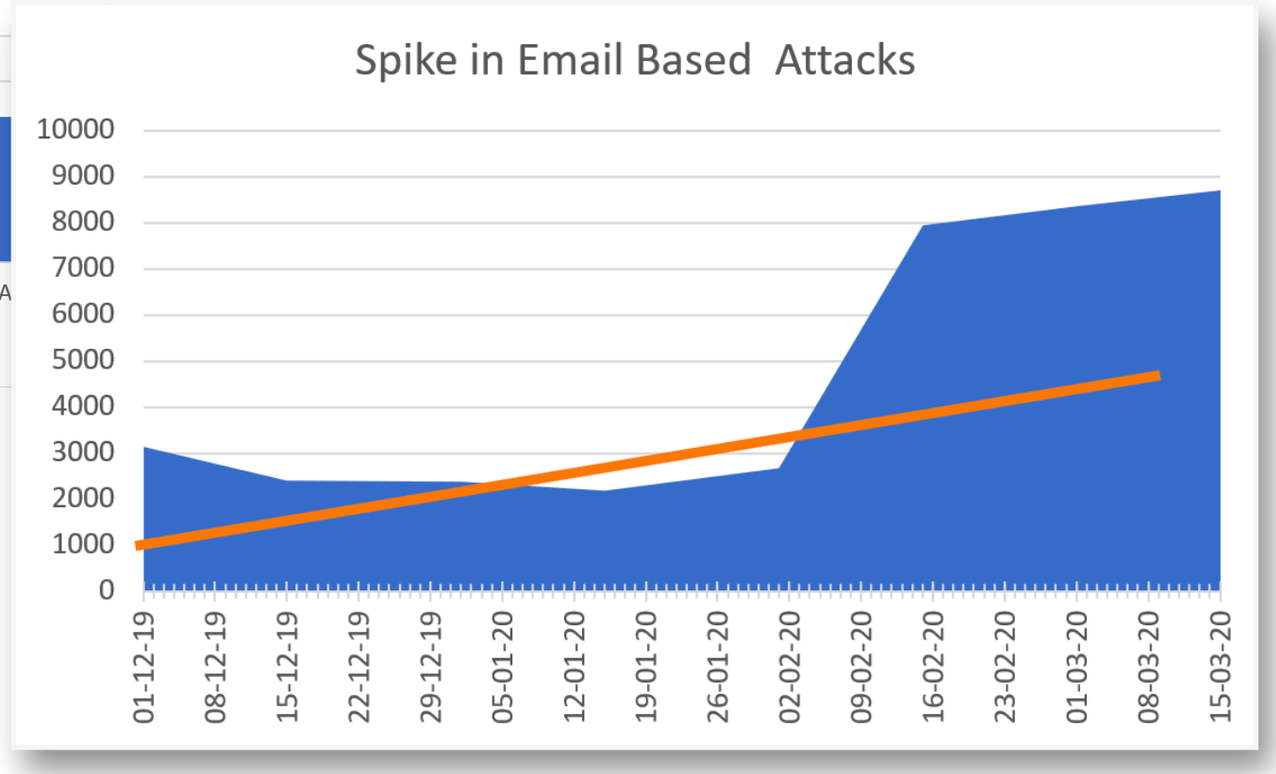
Situation actuelle et précautions

Cyberrisques - Situation actuelle et précautions

Augmentation significative des risques liés aux courriels malicieux

La semaine dernière, une étude réalisée par Cynet a permis de faire la corrélation entre l'augmentation des cas de COVID-19 en Italie et une importante croissance des cyberattaques envers les employés en télétravail.





FÉDÉRATION QUÉBÉCOISE DES MUNICIPALITÉS

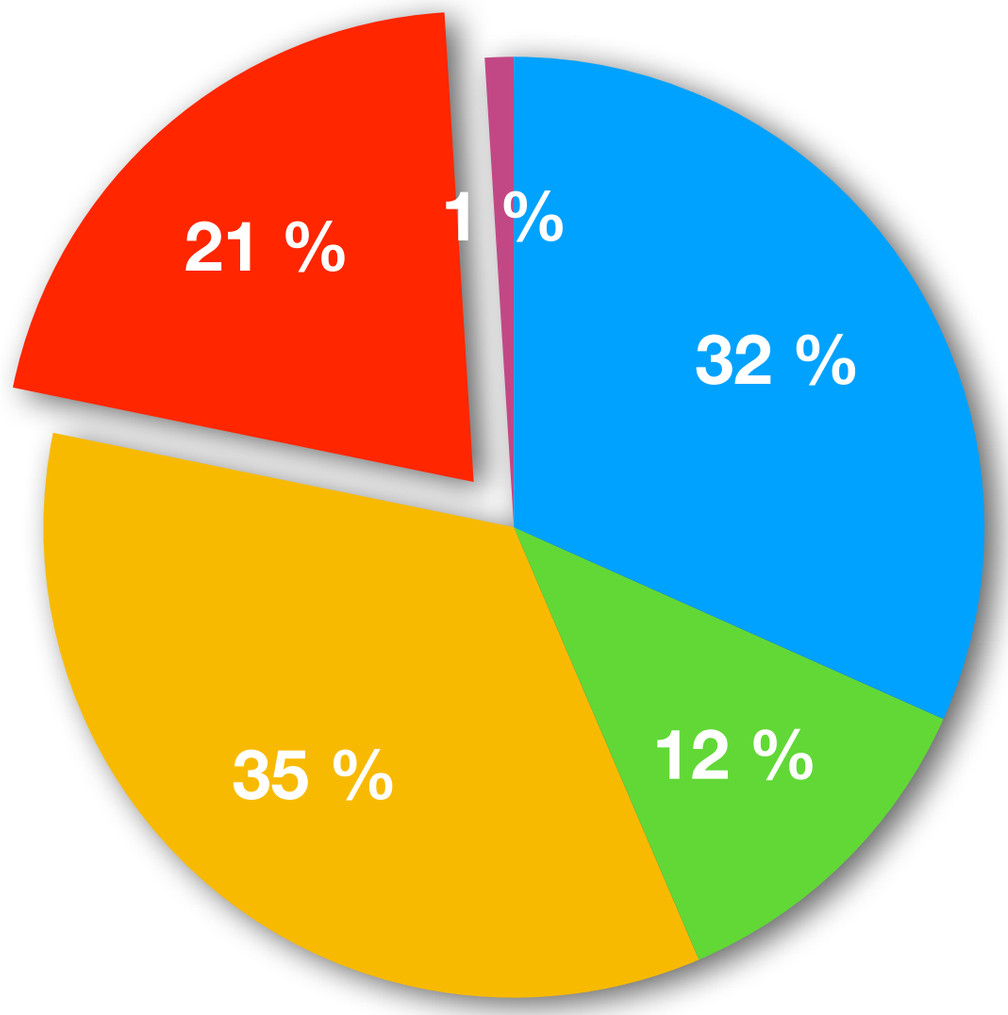
https://www.cynet.com/blog/recent-escalation-in-cyberattacks-in-italy-prove-the-coronavirus-impact-on-cybersecurity-acting-as-a-warning-for-cisos-worldwide/

Cyberrisques - Situation actuelle et précautions

Augmentation significative des risques liés aux courriels malicieux

- Document armé : Macro exécutable
- Document armé : Imitation d'Office
- Courriel avec URL vers un site malicieux
- Courriel contenant un logiciel malicieux
- Autres

Répartition des attaques



FÉDÉRATION QUÉBÉCOISE DES MUNICIPALITÉS

Cyberrisques - Situation actuelle et précautions

Contextes propices et actions aggravantes

- Ressources limitées pour assurer les opérations administratives
  Accès aux logiciels de gestion et maîtrise des processus;

- Mise en ligne services aux citoyens
  Augmentation des interactions par courriel et désir par le personnel de première ligne, de préserver la qualité du service;

- Mise en place accélérée du télétravail;

  - Utilisation d'ordinateurs personnels non protégés par un antivirus, un antipourriel et d'un logiciel d'accès VPN;

  - Partage de mots de passe par courriel.

Cyberrisques - Situation actuelle et précautions

Diminution de la vigilance et augmentation de la prise de risques

Mise à l‘épreuve des compétences informatiques.

- Les personnes expérimentées en informatique étant moins disponibles, les employés moins expérimentés pourraient être poussés à prendre des initiatives dans des sphères qu’ils ne maîtrisent pas.

Par exemple :

- Le paiement de factures à la suite d’une demande pressante par courriel Transfert bancaire, etc.

- Accès aux logiciels de gestion
  Partage des mots de passe en réponse à de faux courriels afin d’assurer la continuité des opérations.

Cyberrisques - Situation actuelle et précautions

Identifier les courriels à risque

Les informations à valider en tout temps

- Les adresses de courriel des contacts publiés dans le site Web ou le logo d'une organisation sont très utiles pour créer une impression d'intimité;
- Les signatures en bas de page réfèrent-elles à des contacts ou des coordonnées connues?
- Est-ce que l'adresse de courriel de l'émetteur réfère au nom de domaine officiel de l'organisation qu'il représente, même au survol de la souris sur l'adresse?
- Est-ce que l'objet de la communication commande une intervention rapide ou immédiate de la part de l'interlocuteur?
- Est-ce qu'il y a un fichier à télécharger ou un lien à cliquer?

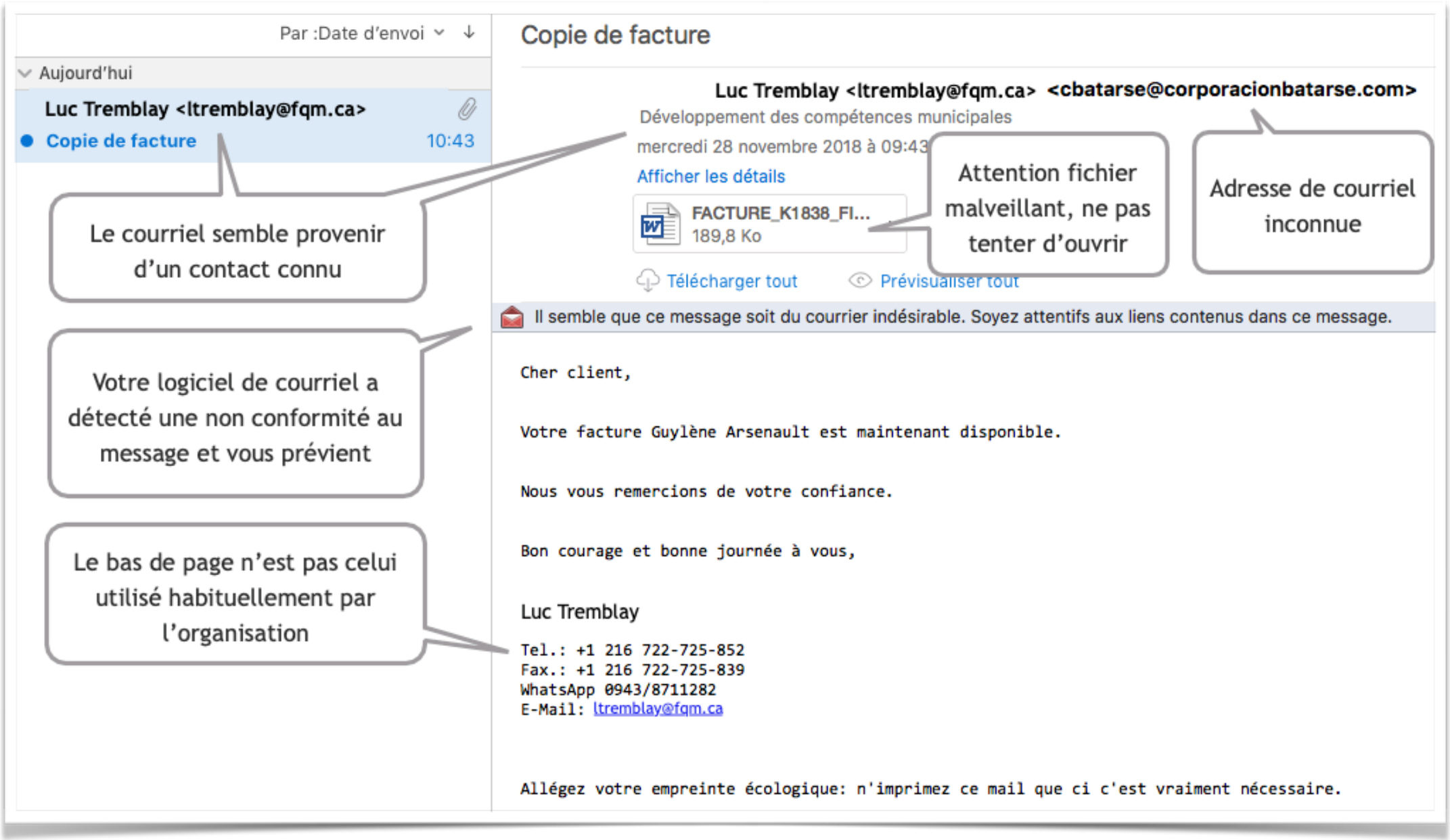
Cyberrisques - Situation actuelle et précautions

Identifier les courriels à risque

Exemple de stratégies utilisées par les cybercriminels:

- Une demande de confirmation de mot de passe pour continuer à avoir accès à un service bancaire ou à un service en ligne;
- Un courriel d'un employé qui dit avoir oublié son mot de passe, comme il travaille de son ordinateur de la maison;
- Un courriel d'un supérieur demandant d'initier une action d'ordre financière;
- Une demande d'aide ou une amorce de conversation d'un contact connu.

Cyberrisques - Situation actuelle et précautions



FÉDÉRATION QUÉBÉCOISE DES MUNICIPALITÉS

Cyberrisques - Situation actuelle et précautions

Que faire devant un courriel à risque

Il est difficile d'être sûr à 100 % que l'on est devant un courriel malicieux. Cependant, dans le doute toutes les mesures de précaution s'imposent.

1. Ne jamais tenter d'ouvrir les documents joints, il est très facile pour un pirate d'imiter un document Word, Excel, PowerPoint et PDF pour cacher un logiciel exécutable EXE malveillant ;

2. Ne jamais cliquer un des liens proposés, ils peuvent activer un téléchargement ou vous diriger vers une page Web contenant des scripts malveillants ;

3. Ne jamais répondre à l'envoyeur, même par curiosité… Vous ne ferez que confirmer aux cybercriminels qu'ils sont sur une bonne piste.
   De plus, ils auront maintenant votre signature et tout ce qu'il faut pour s'attaquer à d'autres cibles en votre nom.

Cyberrisques - Situation actuelle et précautions

Que faire devant un courriel à risque

Mesures immédiates :

- Identifiez le courriel et l'envoyeur comme étant indésirables ;
- Faitez une capture d'écran du courriel ;
- Avisez les TI de votre organisation, ou votre entourage ;
- Détruisez le courriel à la suite du partage de l'information avec les TI.

Cyberrisques - Situation actuelle et précautions

Vos meilleurs remparts

Créer une chaine de communication efficace

- Sensibilisez l'ensemble du personnel sur les risques imminents des courriels malicieux et invitez-les à dénoncer toutes situations suspectes ;
- Identifiez une personne responsable de la cybersécurité ;

Gardez vos logiciels et infrastructure réseau à jour

- Assurez-vous que tous les ordinateurs utilisés pour le télétravail soient à jour et aient des logiciels antivirus, anti-pourriel et accès VPN d'installés ;
- Si votre infrastructure réseau est accessible de l'extérieur, assurez-vous qu'elle est protégée par un pare-feu (Firewall) performant.

CYBERRISQUES

Situation actuelle et précautions

Soyons prudents

Merci