Congrès Événements Attractions Québec
Présenté par Tourisme Centre-du-Québec

7 au 9 NOVEMBRE 2022

PANEL

Cybersécurité : ne négligez pas l'impact humain!

Emeline Manson
CY-Clic
Jacques Lussier
Atypic

Présenté par :

VIRAGE NUMÉRIQUE
Propulsé par ÉAQ

Événements Attractions Québec

VIRAGE NUMÉRIQUE

Propulsé par ÉAQ

Cybersécurité :
Ne négligez pas l'impact humain!

Avec la participation financière de

Québec

Propulsé par

Événements Attractions Québec

Emeline Manson

CY-clic

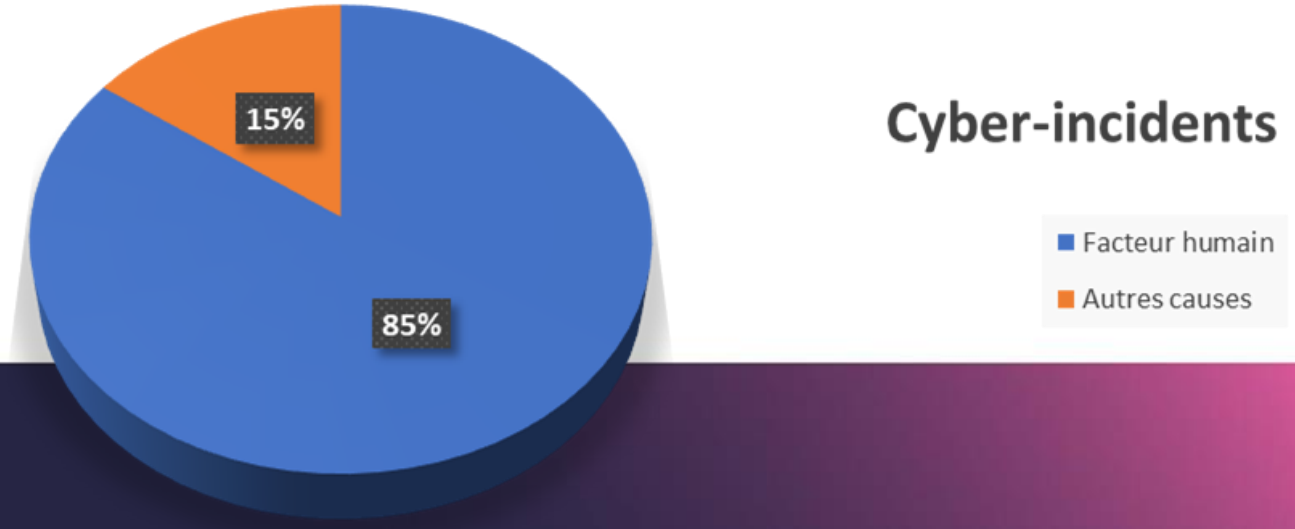
Jacques Lussier

Atypic

Pourquoi l’humain aurait-il un impact en cybersécurité ?

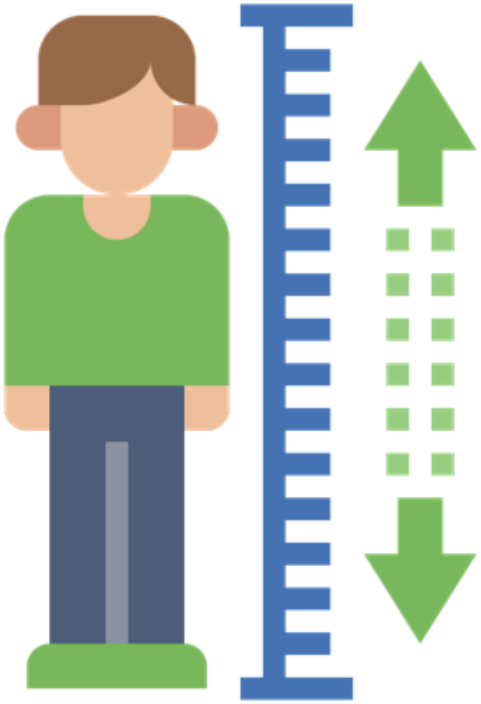
Pourquoi l’humain aurait-il un impact en cybersécurité ?

- Plus de **85 %** des incidents ont comme source l’humain
- **36 %** des employés québécois se disent peu ou pas du tout préoccupés par le vol de données
- **21 %** déclarent avoir été ciblées… mais la plupart ne déclarent pas
- **5.4 M$,** c’est le coût moyen sur 2 années d’un incident (violation de données)
- Près de **25 %** des organisations ne s’en relèvent pas
- **50 %** de plus de cyberattaques chaque semaine sur les entreprises
- **44 %** des violations de données concernent des informations personnelles identifiables



Une TPE ou une PME est-elle autant concernée qu’une plus grande entreprise ?

Une TPE ou une PME est-elle autant concernée qu'une grande entreprise ?



- Souvent plus à risque, car elles ont
  - moins de ressources
  - théoriquement moins de structures
  - infrastructure TI basique
- Important!
  - Hiérarchisation de l'accès aux données
  - La loi 25, nouvelles exigences et responsabilités
- Nouvelle réalité
  - Attaques aléatoires vs. attaques ciblées

De quoi faut-il se méfier dans les communications qu’on reçoit ?

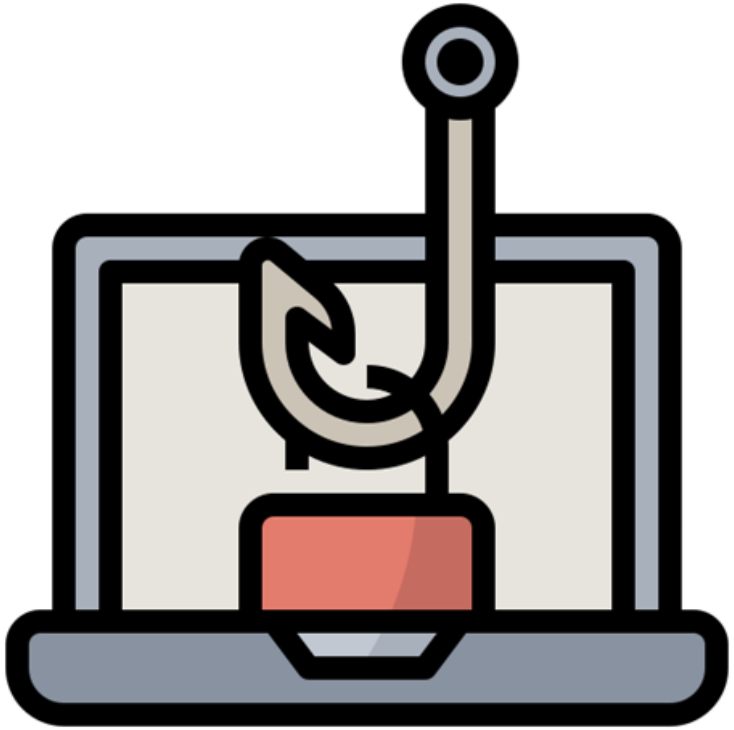
De quoi faut-il se méfier dans les communications qu'on reçoit ?

Quelques moyens

- Liens et pièces jointes
- Courriel, texto, réseaux sociaux
- De plus en plus personnalisée
- Fraude du fournisseur | Fraude du propriétaire

Quelques réalités

- IA utilisée pour exploiter la voix
- Rançongiciel et fuite de données
- Failles zéro-day
- Objets connectés… porte d'entrée insoupçonnée!



Comment sensibiliser les équipes ?

Comment sensibiliser les équipes ?

Le secret
Prévention, sensibilisation et planification

Des réalités, des réactions, des planifications…

- Chaque personne peut devenir un point d'entrée
- Peur d'être blâmé en cas d'erreur
- Préparer le terrain en cas d'attaque - qui fait quoi ?
- Plan de contingence à mettre à jour
- Politique de cybersécurité

Source: Atypic

Comment sensibiliser les équipes ?

Le secret
Prévention, sensibilisation et planification

Des réalités, des réactions, des planifications…

- Sensibiliser vs. Apporter des solutions pratiques
- Adhésion au changement
- Que les équipes se sentent concernées
- Formation synchrone vs. asynchrone
- Formation continue
- Simulation d’hameçonnage

La sensibilisation est un travail continu!

Quel a été l’impact du télétravail sur les cyberattaques ?

Quel a été l'impact du télétravail sur les cyberattaques ?

Les particuliers aussi ciblés, car ce sont de potentiels points d'entrée pour les cybercriminels

- Augmentation des attaques
- Faux sentiment de sécurité
- Vos équipements à la maison sont-ils bien paramétrés ?
- Partage réseau avec la famille

À ne pas négliger…

- Plateformes de collaboration en ligne
- Accès direct à l'entreprise en ligne
- Utilisation du VPN

63 % des entreprises au Canada ont constaté une augmentation des cyberattaques ciblées depuis qu'elles se sont tournées vers le télétravail.

- Rapport de Proofpoint 2021

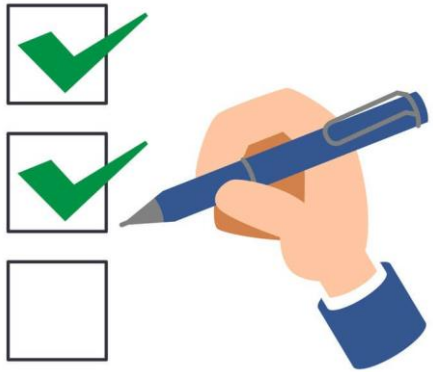
20 % des organisations ont été victimes d'une cyberattaque causée par un collaborateur en télétravail depuis le début de la pandémie.

- Rapport de Malwarebytes

Quelles seraient des solutions et bonnes pratiques rapides à mettre en place ?

Quelles seraient des solutions et bonnes pratiques rapides à mettre en place ?

- Bonne gestion des accès
- Processus de sauvegardes
- Principe de l'accès minimal:
  Qui doit avoir accès à quoi?
- Bonne gestion des mots de passe
- Mot de passe robuste, unique et 2FA
- Informations sensibles par courriel



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

› Learn about our methodology at hivesystems.io/password

Quelles seraient des solutions et bonnes pratiques rapides à mettre en place ?

Rigueur et quelques outils seront vos alliés !

À partager :

Outil de gestion : Liste des rôles et accès

LISTE DES RÔLES ET ACCÈS

Ce gabarit fait partie des ressources offertes par CY-clic.

Étape 1 : Faites la liste des comptes dont dispose l'entreprise. Pour vous aider, visiter : cet outil
Étape 2 : Énumérer les employés de votre organisation. N'oubliez pas les rôles temporaires : stagiaires, pigistes, comptable, partenaires, etc.
Étape 3 : Noter lorsqu'il s'agit d'un compte partagé, c'est-à-dire, qu'il n'y a qu'un seul identifiant et mot de passe, que les équipes se partagent.
Étape 4 : Valider si les mots de passe sont à changer pour chacun des membres de l'équipe.
Étape 5 : Valider si le double facteur d'authentification est à activer pour chacun des membres de l'équipe.
Étape 6 : Une journée à la fois, apporter les correctifs nécessaires. Fixer 10 minutes cybersécurité à chaque réunion d'équipe ; les changements pourraient être fait à ce moment-là!

	FACEBOOK	LINKEDIN	INSTAGRAM	YOUTUBE	MICROSOFT	MICROSOFT ADMIN	GOOGLE	DROPBOX	ZOOM	SKYPE	ACOMBA	QUICKBOOK	ZOHO	HUBSPOT	MAILCHIMP	CANVA	CALENDLY	TRELLO	YAPLA	COMPTE DE BANQUE	SERVICE DE PAIE	ASSU COLL
RÔLE 1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
RÔLE 2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
RÔLE 3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
RÔLE 4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
NOTE			compte partagé	compte partagé					compte partagé		compte partagé				compte partagé	compte partagé						
MOT DE PASSE À CHANGER																						
RÔLE 1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
RÔLE 2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
RÔLE 3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
RÔLE 4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
2FA																						
RÔLE 1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
RÔLE 2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
RÔLE 3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
RÔLE 4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	

Des questions ?