Vos conférenciers

Jérôme Martel
Dir. Développement & Partenariats
Conférencier Cybersécurité & IA

Rosemarie Labrecque
Dir. Solutions d’affaires
Stratège Cybersécurité & IA

LA CYBERCRIMINALITÉ EN 2025

MENACES ET RISQUES

TECHNOLOGIE **PROCESSUS** **HUMAIN**

LES CYBER-ATTAQUES À TRAVERS LES **ANNÉES**

Sollio Groupe Coopératif victime d'un rançongiciel, une de ses filiales **Olymel** victime d'une brèche de données via un logiciel malveillant

Une petite **ferme porcine** en Ontario a été victime d'une attaque par ransomware orchestrée par des activistes.

2021

2022

2023

2024

L'UPA victime d'un rançongiciel qui a affecté les systèmes informatiques **et Maple Leaf** victime d'une attaque qui aura coûté plus de 23M$

Agropur victime d'une brèche de données **Federated Co-ops** victime d'un rançongiciel

FAIBLE VIGILANCE : GRANDS RISQUES

Le géant québécois de l'agroalimentaire Agropur a été la cible d'une cyberattaque dans les derniers jours.

cyberpirates menacent de publier dans trois jours lui ont volée.

Attaque informatique majeure chez Olymel

L'informatisation de l'agriculture ouvre la porte à la cybercriminalité

Cyberattack knocks out systems

Threat of agriculture-related cybercrime is rising

des engins agricoles pou

er l'agricultu

L'Union des producteurs agricoles (UPA) est ciblée depuis dimanche par une attaque par rançongiciel qui touche l'ensemble de ses systèmes informatiques.

Activists target Ont. hog farm with ransomware

Cyberattack cost Maple Leaf Foods at least CA$23 million

La cybersécurité et votre entreprise agricole

La cybersécurité, un véritable enjeu pour le secteur agroalimentaire

30 000 agriculteurs victimes d'une cyberattaque

Les éleveurs de porcs victimes d'une cyberattaque

Cyberattack kn

(Montréal) La cyberintimidation de la part d'activistes véganes est un facteur de stress et de détresse de plus en plus important pour les agriculteurs,

Hacker des engins agricoles pour paralyser l'agriculture, une menace pour la sécurité alimentaire

Piratage informatique : l'agriculture de plus en plus sous la menace

landes de rançon...

es pirates

Arnaques, demandes de rançon... Les pirates n'épargnent plus les agriculteurs !

Cyberattack knocks out systems at Canada's Federated Co-op stores

LA CYBERSÉCURITÉ, C'EST QUOI ?

Toutes les actions visant à **identifier, comprendre, contrôler et réduire** les risques de cybersécurité.

Humain

Être conscient des menaces.
Reconnaître les indices.
Utiliser les meilleures pratiques.

Processus

Gestion des informations sensibles.
Politique de cybersécurité.
Plan d'intervention.
Etc.

Technologie

Utilisation d'outils de sécurité avancés.
Utilisation de technologies adaptées.
Applications à jour et sécurisées.
Faire appel à des experts.

PLAN DE LA SÉANCE

1. Les techniques de cyber-attaques
2. La menace : L’écosystème
3. Qui sont les cyber-criminels
4. Le dark web
5. Les techniques pour créer un bouclier
6. La gestion d’un incident
7. Quelques statistiques
8. Période de questions (virtuelle)

LES QUATRE ATTAQUES LES PLUS FRÉQUENTES

Rançongiciels (ransomware)

Chiffrement des données critiques et demande de rançon. Des sauvegardes adéquates sont essentielles pour réduire les conséquences.

Exploitation de vulnérabilités

14 % des cyberattaques parviennent à s’infiltrer via des logiciels obsolètes ou non mis à jour.

LES QUATRE ATTAQUES LES PLUS FRÉQUENTES

Fraudes alimentées par l’IA

Les cybercriminels utilisent **l’intelligence artificielle** pour créer des fraudes extrêmement convaincantes. Cela inclut le **vishing.**

L’hameçonnage

Les cybercriminels **incitent** des individus à **divulguer** des **informations confidentielles** ou à **installer des logiciels malveillants.**

EXEMPLE D'HAMEÇONNAGE

Canaux : tous les moyens de communication

Objet : Inspection sanitaire urgente – MAPAQ
Expéditeur : inspection@mspaq-qc.com

Bonjour,

Dans le cadre d'un audit régional de conformité, le ministère vous demande de **remplir le formulaire en ligne** suivant avant **demain 18 h** pour éviter des pénalités.

Ce formulaire est obligatoire et fait suite à des ajustements en matière de biosécurité pour les exploitations agricoles.

➡ Accéder au formulaire officiel MAPAQ

Merci de votre collaboration,
Service des inspections agroalimentaires
Gouvernement du Québec

Exemple : Faux site imitant le portail du MAPAQ

L'attaquant prétend être la MAPAQ afin de voler des renseignements sensibles, accéder aux services de messageries, télécharger des documents sensibles ou installer un logiciel malveillant.

Est-ce que vous devez poser une action?

LA MENACE : L'ÉCOSYSTÈME

Votre écosystème

Vos employés, collègues, fournisseurs, clients, enfants, petits-enfants, conjoints(es), voisins(es), amis(es), bref tous les gens avec qui vous discutez sur le web.

Risque d'occurrence d'une menace

Très élevé : tous les moyens de communication (courriels, appels, textos, applications, jeux et sites d'achat en ligne, etc.)

UN CONCEPT : ZERO TRUST

QUI SONT LES CYBER-CRIMINELS ?

Les déguisés : Ils se font passer pour des personnes légitimes.

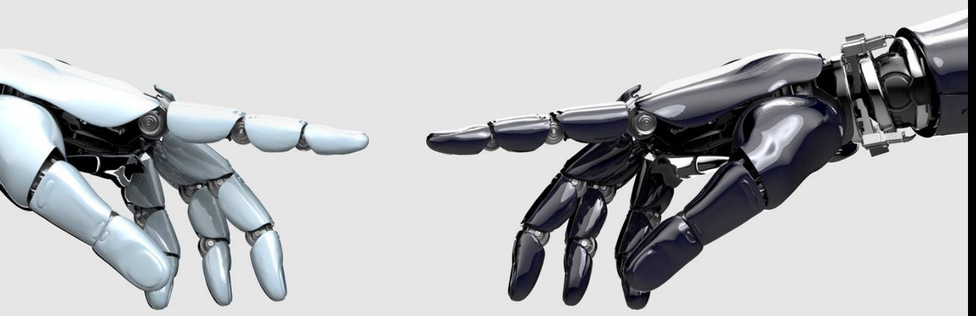
Les ingénieurs sociaux : Experts en manipulation psychologique, ils exploitent la nature humaine.

Les espions : Ils interceptent et modifient les communications entre deux parties.

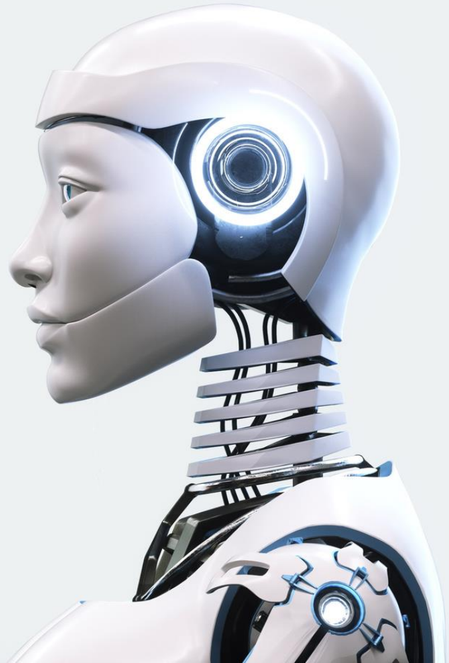
Les techniciens : Spécialistes en failles de sécurité, ils exploitent des vulnérabilités dans vos appareils.

Les hacktivists : des individus qui utilisent le piratage informatique à des fins politiques, idéologiques ou sociales.

Les pros de l’IA : utilisent l’IA pour créer des courriels convaincants, imiter des images, des voix ou des sites web de manière presque parfaite.



L'ARRIVÉE DE L'IA



1. Personnalisation des attaques

Imitation des tons /styles de communication, etc.

2. Automatisation des attaques

Envoi de courriels en quantités massives.

3. Analyse rapide

Vastes quantités de données personnelles disponibles en ligne.

4. Rapidité de création

Sites ou applications frauduleuses.

5. Évolution des menaces

Reproduction de la voix, des individus sur vidéo, etc.

LE DARK WEB, C’EST QUOI?

C’est une **section clandestine d'Internet**, propice à des activités confidentielles, **souvent** même **illégales**, due au niveau d’anonymat élevé qu’il octroie aux utilisateurs, ce qui **facilite le commerce de biens et services illicites**, par exemple relativement aux **renseignements personnels**.

Arrivée de l’ère moderne du Dark Web en 2002 (TOR), financé en grande partie par le gouvernement américain dans un objectif positif.

AVEZ-VOUS DÉJÀ ÉTÉ **COMPROMIS**?

Oh no — pwned!

Pwned in 7 data breaches and found no pastes (subscribe to search sensitive breaches)

Deezer: In late 2022, the music streaming service Deezer disclosed a data breach that impacted over 240M customers. The breach dated back to a mid-2019 backup exposed by a 3rd party partner which was subsequently sold and then broadly redistributed on a popular hacking forum. Impacted data included 229M unique email addresses, IP addresses, names, usernames, genders, DoBs and the geographic location of the customer.

Compromised data: Dates of birth, Email addresses, Genders, Geographic locations, IP addresses, Names, Spoken languages, Usernames

ClickASnap: In September 2022, the online photo sharing platform ClickASnap suffered a data breach. The incident exposed almost 3.3M personal records including email addresses, usernames and passwords stored as SHA-512 hashes. Further, a collection of paid subscriptions were also included and contained names, physical addresses and amounts paid.

Compromised data: Email addresses, Names, Passwords, Physical addresses, Purchases, Social media profiles, Usernames

';--have i been pwned?

RENFORCER VOTRE CYBER-RÉSISTANCE

LES BONNES PRATIQUES

- Activez l’authentication à double facteurs.
- N’utilisez pas votre adresse courriel professionnelle pour des fins personnelles (vice-versa).
- Effectuez vos mises à jour.
- Limitez les autorisations accordées aux applications.
- Effectuez une double verification de l’identité de vos interlocuteurs.
- Évitez les connexions Wi-Fi publiques, surtout celles non sécurisées.
- Créez des mots de passe forts (p.ex.C0mpl3xP@ssw0rd!).

Le temps nécessaire à un pirate pour découvrir votre mot de passe selon sa composition

Nombre de caractères	Uniquement des chiffres	Uniquement des lettres minuscules	Des lettres minuscules et majuscules	Des chiffres, des lettres minuscules et majuscules	Des chiffres,des lettres minuscules, majuscules et des symboles
4	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
5	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
6	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
7	Instantanément	Instantanément	1 seconde	2 secondes	4 secondes
8	Instantanément	Instantanément	28 secondes	2 minutes	5 minutes
9	Instantanément	3 secondes	24 minutes	2 heures	6 heures
10	Instantanément	1 minute	21 heures	5 jours	2 semaines
11	Instantanément	32 minutes	1 mois	10 mois	3 ans
12	1 seconde	14 heures	6 ans	53 ans	226 ans
13	5 secondes	2 semaines	332 ans	3k ans	15k ans
14	52 secondes	1 an	17k ans	202k ans	1M ans
15	9 minutes	27 ans	898k ans	12M ans	77M ans
16	1 heure	713 ans	46M ans	779M ans	5 billions d’ans
17	14 heures	18k ans	2 billions d’ans	48 billions d’ans	380 billions d’ans
18	6 jours	481k ans	126 billions d’ans	2 trillions d’ans	26 trillions d’ans

GESTION D'UN INCIDENT CYBER

Un incident cyber, c’est quoi?

- Un vol d’identité
- Tentative d’hameçonnage réussie
- Contraction d’un virus
- Détournement de courriels
- Une fraude
- Un crime contre la personne
- Un bris matériel ou une panne
- Un accès non autorisé à une base de données

Comment réagir ?

1. Cessez l’utlisation de l’appareil immédiatement.

2. Ne tentez pas de régler ou de camouffler la situation.

3. Avertissez votre fournisseur de service, un professionnel TI ou toute personne en autorité.

4. Mettez votre plan d’intervention en action

5. Suivez les consignes qui vous seront communiquées (plainte, police, etc.)

QUELQUES STATISTIQUES

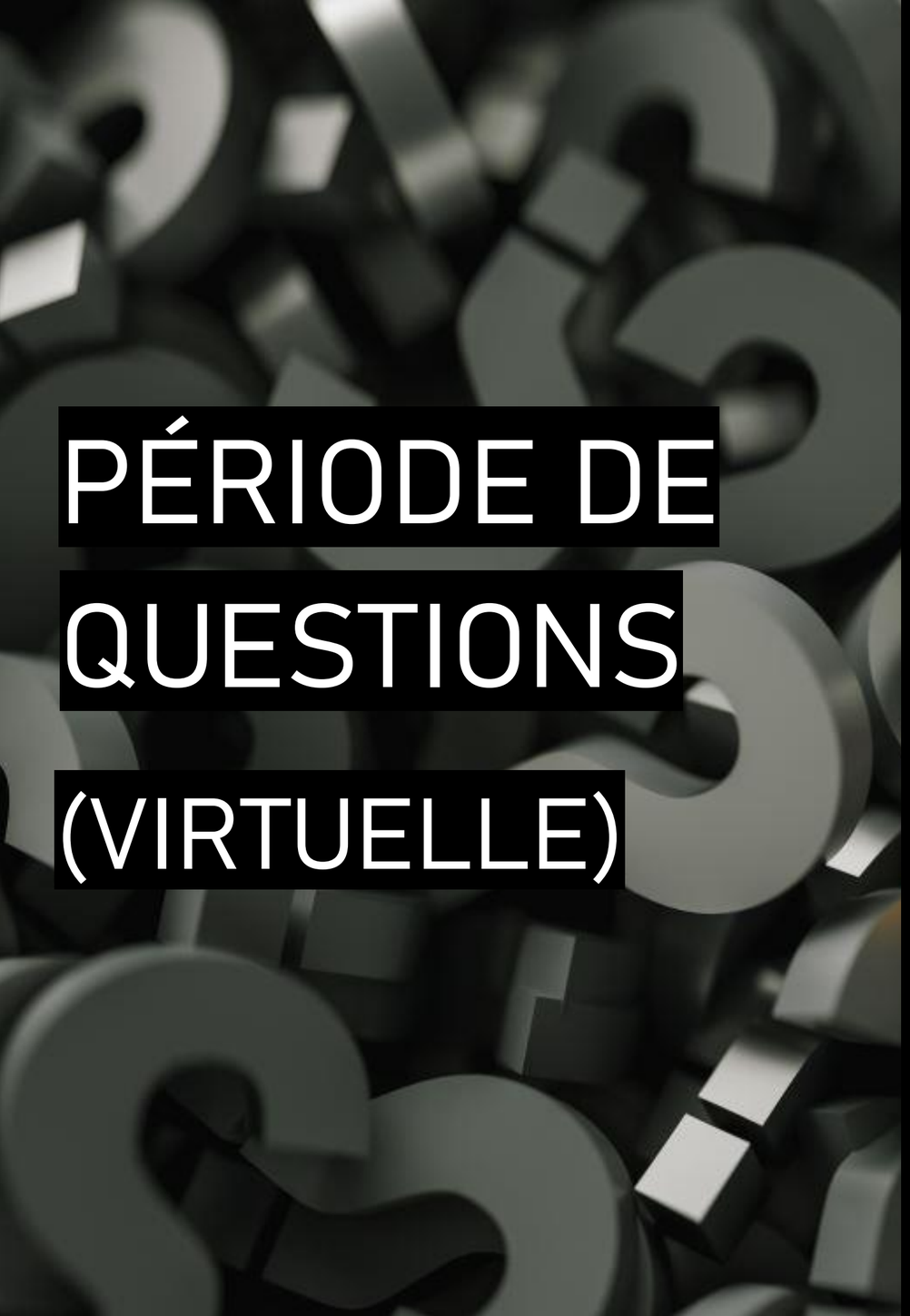
1,2G$ en pertes déclarées en 2023 reliées aux cybercrimes.

6.6 millions d’activités potentiellement malveillantes sont bloquées chaque jour par le centre de la sécurité des télécommunications (CST).

80% des producteurs agricoles n’ont pas de plan d’intervention en cas d’incident de cybersécurité.

36 % des professionnels de l’agroalimentaire ont été touchés par des cyberattaques au cours de l’année écoulée.

Parmi les entreprises affectées, 70 % ont subi des impacts significatifs sur leur production ou leur organisation interne.



PÉRIODE DE QUESTIONS (VIRTUELLE)

Jérôme Martel
Dir. Développement & Partenariats
Conférencier Cybersécurité & IA

Rosemarie Labrecque
Dir. Solutions d’affaires
Stratège Cybersécurité & IA