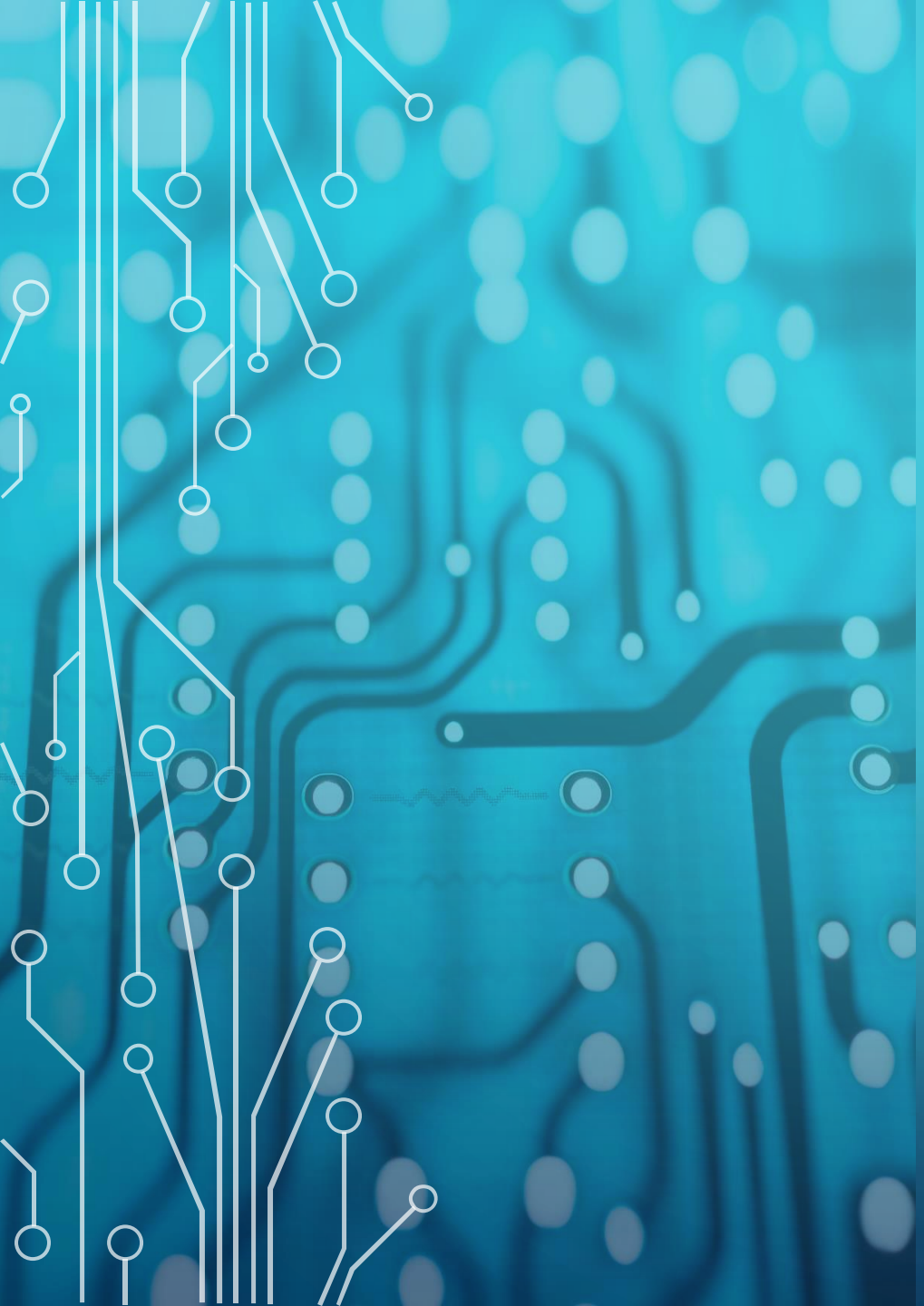
SENSIBILISATION CYBERSÉCURITÉ



PRÉSENT ET PRÉOCCUPANT

- On en entend de plus en plus parler.
- On connait des entreprises proches.
- On reçoit des choses bizarres mais d'autres fois ce sont des liens totalement fiables qui sèment le doute.
- Suis-je une cible ?
- Suis-je bien protégé.e ?

QUI EST LE.LA PIRATE?




AVANT :




- Veut relever des nouveaux défis
- Trouver la brèche de sécurité
- Se prouver auprès de la communauté
- Code du pirate
- Peu d'organisation

AUJOURD'HUI :

- Peut être n'importe qui
- Travaille pour nourrir sa famille/gagner sa vie
- Organisations
- Procédures comme vos tâches quotidiennes
- Impersonnel, à grande échelle

Le pirate ou la pirate ne s'acharnera pas sur vous 3 semaines pour vous soutirer 1000$ mais acceptera bien de ramasser un 1000$, en passant, sans trop d'efforts.

QUELS SONT LES PIÈGES ?

- Social engineering & Phishing (hameçonnage)
- L'injection de malware ou virus
- Briser le mot de passe « Cracking »
- Les environnements auxquels on ne porte plus attention (vulnérables)
- DDoS

Pourquoi ?

Accéder aux données, voler de l'information pour revente ou espionnage, rançon, causer des dommages, etc.

SOCIAL ENGINEERING & PHISHING (HAMEÇONNAGE)

- Consiste à essayer d'attraper une victime, parfois ciblée dans une organisation, et d'essayer de lui soutirer des informations personnelles. C'est souvent un courriel ou un site web
  - Personne qu'on connait
  - Un fournisseur avec une facture à payer
  - Une cause noble

3.4 milliards de courriels d'hameçonnage enregistrés en 2022

Ne donnez jamais d'information privée dans vos courriels.
Penses-y a deux fois avant d'ouvrir un attachement et dans le doute, abstenez-vous.

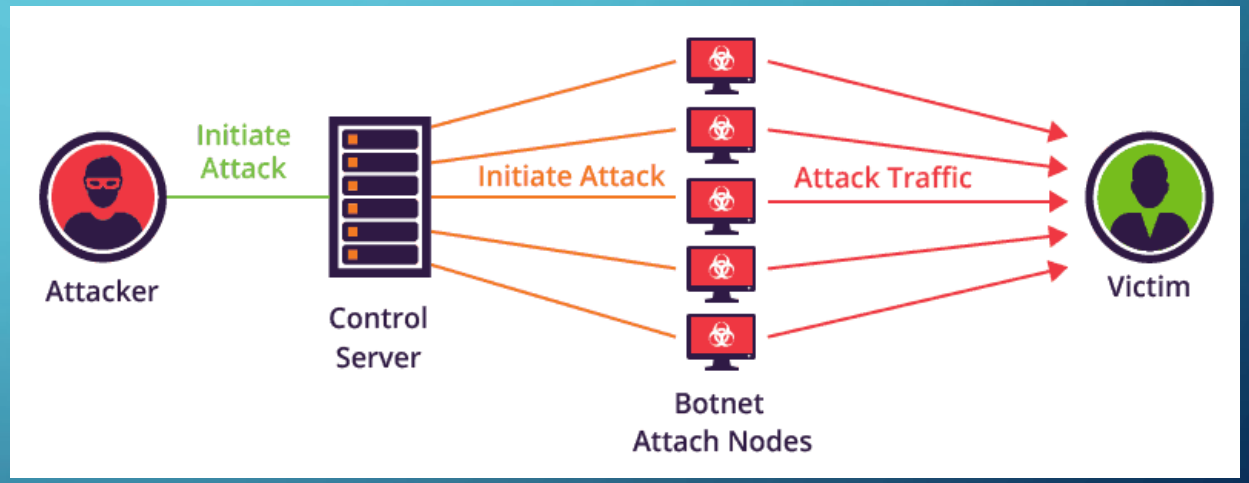
L'INJECTION DE MALWARE OU VIRUS.

- Une clé USB, un disque, un courriel peut sembler inoffensif.
  - Seulement connecter la clé est suffisant pour déclencher le virus.
    - KeyLogger
    - Vol de cookies (Spyware)
    - Ransomware
    - Chevaux de Troie
    - Adware et redirects
    - Rogues Applications

Tenez vos antivirus à jour.
N'utilisez pas de clé USB perso pour le travail et vice versa.
Ne pensez même pas aux clés USB des inconnus.

DDOS (DISTRIBUTED DENIAL OF SERVICE).

- C’est une prise de possession d’un groupe d’ordinateur pour attaquer une cible simultanément.
  - Hacktivism
  - Extorsion
  - Compétition entreprise ou personnel
  - Cyber guerre



Tenez vos antivirus à jour.

BRISER LE MOT DE PASSE « CRACKING »

- Le keylogging et le vol des cookies
- Force brute
- Mot de passe le plus utilisé : 4 929 113 (Password)
- La fuite de mot de passe (essais sur toutes les autres plateformes)

Les mots de passes complexes et l'authentification multifacteur
par exemple sont des façons de contrer ces attaques
à condition de rester vigilant.e. 1Password, Keeper, NordPass

LES ENVIRONNEMENTS AUXQUELS ON NE PORTE PLUS ATTENTION

- Avec le télétravail, il est intéressant d'entrer dans les maisons et d'espionner les allées et venues
  - Google Home, Domotique, vieille ordi, router, frigo, télévision intelligente, smart phone, smart watch, etc.
- WAP (antenne relais n'existe pas seulement dans les films d'espionnage)
- WIFI publiques (qui est à l'écoute ?)

Tenez vos équipements à jours
Utilisez un VPN fiable dans les environnements à risque ex: NordVPN
Ayez un antivirus intelligent et à jour.

PROTECTIONS

Antivirus (types):

+ Signature
+ Comportement (vulnérabilité moindre aux 0-days)
+ Apprentissage automatique

Pare-feu, Contrôle web, VPN (en environnement inconnu)

Gestionnaire de mot de passe

+ Garde les mots de passe sécurisés et cryptés
+ Génère pour vous les mots de passe (pas de répétitions)
+ Centralisé, risque d'accès

PROTECTIONS

Sauvegardes physiques et/ou cloud

Protection courriel

- SPF (sender policy record) protège le domaine contre spam, spoofing et phishing
- DKIM (DomainKeys Identified email) confirme l'authenticité de l'envoyeur et de son contenu. Qu'il n'a pas été altéré.
- DMARC (Domain-based Message Authentication, Reporting and Conformance) contraint l'envoi de courriel aux personnes autorisées seulement. Évite la fraude du président par exemple.

SE PRÉPARER POUR QUAND ÇA ARRIVERA:

Sauvegardes physiques ou cloud

- Données courantes
- Courriels
- Comptabilité
- Site web

Sécuriser les mots de passe (crypter, multifacteur, entreposer)

- Plan de redondance?
- Plan de remise en route?

➡ Définir le temps acceptable, les données essentielles

- Suivre, réviser et tester régulièrement le plan
- Diffusion de l'information (loi 25)

RESTEZ VIGILANT.E

Le but n'est pas de vous faire peur, mais de vous sensibiliser sur les menaces !

Il faut rester vigilant.e comme quand vous barrez vos portes de maison avant de partir. Comme quand vous évitez de laisser votre voiture sur le neutre dans une pente. Comme quand vous mettez un casque en Ski Doo.

Vous doutez d'un site ou d'un courriel ?

Abstenez-vous !

Vous trouvez que ça a l'air louche ? Ça vaut la peine de **revérifier** !

Jasette cybersécurité – 27 septembre 2023

LISTE DE RÉFÉRENCES

Au cours de la jasette, des groupes susceptibles d'accompagner les OBNL dans la gestion de leur cybersécurité ont été mentionnés. Une recherche internet complète cette liste.*

- Des OBNL au service d'OBNL : SynergiTIC, INSERTECH
- Certaines entreprises informatiques offrent un service d'audit en cybersécurité :
  - PR2 Experts Conseils
  - Solulan,
  - MicroAge,
  - Fleetinfo,
  - Data Next Step,

    Voir l'article réalisé par Data Next Step en collaboration avec Espace OBNL : « 10 astuces simples (et peu coûteuses) pour améliorer la sécurité de vos données dans votre OBNL ».
- La Geek Squad de Best Buy (pour des services aux particuliers)
- La suite Pureview de Microsoft

Autres liens d'intérêt :

Tiré du site CPA Canada : 20 questions que les administrateurs devraient se poser en cybersécurité.

Le Centre antifraude du Canada répertorie différentes fraudes, lorsqu'on veut faire des vérifications sur de possibles tentatives malveillantes.

Espace OBNL : Capsule technique #41 - Cybersécurité en OBNL: y accordez-vous assez d'importance?

*Cette information ne constitue en aucun cas une recommandation de la Fondation J. Armand Bombardier, mais bien un partage de ressources.