Introduction à la sécurité informatique

La sécurité des systèmes d'information
dans la vie quotidienne
et la vie professionnelle

Plan de la présentation

- Pourquoi parler de sécurité ?
- Les principaux risques et dangers
- Les bonnes pratiques
- Que faire en cas de problème ?

A) Pourquoi parler de sécurité informatique ?

- Nous utilisons des systèmes d'information tous les jours
- Menaces multiples
- Ce n'est pas uniquement l'affaire de spécialistes
- Nos pratiques ont des conséquences

Systèmes d'information

- Ordinateur, serveur
- Smartphone
- Distributeur de billets TPG/CFF
- Bancomat
- Appareils connectés
- etc.

Menaces multiples

- Pour vous-mêmes
- Pour vos proches
- Pour votre entreprise, association
- Pour l'État où vous vivez

Qui s'occupe de sécurité ?

- Les développeureuses : systèmes, logiciels
- Les responsables de sécurité internes
- Les délégué·es à la protection des données
- Les personnes mandatées, partenaires : entreprise externe, indépendant
- Chaque utilisateurice final·e

Un problème de sécurité...

- empêche de travailler
- fait perdre du temps, des ressources
- coûte de l'argent
- met en danger des personnes
- peut avoir des conséquences légales

B) Les principaux risques et dangers

- Qui nous veut du mal ?
- Comment peut-on nous atteindre ?
- Le phishing
- Les pièces jointes
- Les autres dispositifs
- L'ingénierie sociale

Qui sont les hackers ?

- Indépendants et petits groupes
- Grands groupes organisés (quels objectifs?)
- Employé·es, partenaires indélicats
- Grandes organisations criminelles (~mafias)
- Gouvernements

Comment se passe une attaque ?

- Repérage des cibles
- Prise d'information, exploitation de failles
- Prise de contact, demande d'action
- Infiltration (logiciel, bout de code…)
- Déclenchement (copie d'information, cryptage du disque, diffusion de virus, utilisation indésirée de votre ordinateur…), persistance
- Exploitation des informations obtenues
- Nettoyage

On vous connaît !

- Informations sur l'entreprise (site web, moteur de recherche, registre du commerce, wikipedia...)
- Réseaux sociaux, petites annonces, forums, blogs...
- Vos dispositifs laissent des traces (smartphone comme point d'accès…)
- D'autres parlent de vous ou ont des informations sur vous
- Vous laissez des traces en naviguant (cookies, adresse IP, sessions...)
- Les moteurs de recherche enregistrent bien plus que les mots clés

Hameçonnage (phishing)

- Technique frauduleuse pour tromper une personne et l'amener à communiquer des informations personnelles
- Faux : message, site, SMS, appel téléphonique, information sur les réseaux sociaux
- Lien ou invitation à visiter un site
- Donner des informations personnelles

Pièces jointes

- Virus, cheval de Troie, ver
- Documents contenant des macros (programmes)
- Page web contenant un formulaire
- Autres : économiseur d'écran qui se fait passer pour un PDF, jeu rigolo, vidéo, ...

Périphériques

- Clé USB
- Disque dur externe
- Carte SD
- Faux réseau Wi-Fi

Ingénierie sociale

- Utiliser des éléments de psychologie (PNL, langage corporel, biais humains…) pour vous atteindre, ou obtenir des informations
- Mêmes techniques que : la vente (persuasion), la magie (détourner l'attention), les avocat·es (éloquence, bonne connaissance du sujet), la comédie (jouer un rôle)...
- Principaux leviers utilisés : respect de l'autorité, besoin de reconnaissance, réciprocité, urgence/stress, appât du gain

C) Les bonnes pratiques

- Environnement
- Système et protections de base
- Réseaux sociaux
- Web
- E-mail
- Mots de passe

Environnement de travail

- Attention à ce qu'on laisse traîner : impressions, post-it, papiers sous le clavier…
- Ranger le bureau, mettre les documents confidentiels ou importants sous clé
- Ne pas connecter des dispositifs qu'on trouve (clés USB, cartes SD...)

Système

- Tenir son système et ses logiciels à jour
- Devoir entrer un mot de passe de session
- Le disque peut être crypté
- Ne pas travailler avec droits admin
- Ne pas partager les mots de passe
- Mettre en veille (avec mot de passe) quand on quitte le poste
- Utiliser des dispositifs de sécurité (antivirus, firewall, proxy VPN…)
- Faire des sauvegardes régulières, vérifier l'intégrité, tester la restauration
- Éviter les gratuiciels (même séduisants : CCleaner, antivirus...)

Réseaux sociaux

- Réfléchir à ce qu'on publie (informations, photos de vacances, noms des animaux domestiques…) : les vies privées et professionnelles ne sont pas très cloisonnées
- Rechercher des informations sur soi (il est très difficile de retirer des informations d'internet!)
- Faire attention à ce que d'autres publient sur nous

Web : comment s'y retrouver ?

- Quelle sécurité sur un site web ?
- Comment vérifier l'authenticité ?
- Puis-je faire confiance aux formulaires ?
- Téléchargements
- Moteurs de recherche
- Enregistrer les mots de passe ? NON !
- Surveiller les fuites de données
- Utiliser des dispositifs et sites respectueux de la vie privée

E-mail : questions à se poser

- Est-ce que j'attends un message comme celui-ci ? ou est-il non sollicité ?
- Quelle est sa provenance ? puis-je la vérifier ?
- Que me demande-t-on ?
- La/les pièces jointes semblent-elles légitimes ?
- Comment s'adresse-t-on à moi ?

E-mail : actions

- Dans le doute : s'abstenir (de cliquer sur les liens, d'ouvrir les pièces jointes, de transmettre des informations, de rediriger le message…)
- Dans le doute : vérifier (en allant voir ou en téléphonant à la personne), envoyer à la/au responsable IT
- Si ça semble légitime, mieux vaut aller sur le site en question avec ses propres habitudes (bookmarks) que cliquer sur un lien proposé
- Utiliser un filtre (antispam) et «documenter» les messages

Ingénierie sociale

- Repérer les biais qui vont nous faire déraper : sentiment d'urgence, références à plusieurs personnes connues, interlocuteurice autoritaire, demande étrange, sentiment d'être redevable envers une personne, sentiment que quelque chose cloche
- Valider l'identité de la personne
- Se poser des questions, en poser à la personne
- Décliner les demandes inhabituelles
- Noter les détails de l'interaction (heure, lieu, noms mentionnés…)
- Ne **jamais** donner un mot de passe

Parlons mots de passe (1/2)

- Un mot de passe est personnel !
- Il devrait contenir **au minimum** 12 caractères, dans 4 classes (minuscules, majuscules, chiffres, caractères spéciaux)
- Utiliser des mots de passe différents, ne pas associer les mêmes adresses avec les mêmes mots de passe
- Ne **jamais** utiliser le mot de passe associé à l'adresse, sur un site
- Activer le changement de mot de passe par défaut (tous les 6 mois, tous les ans…), si possible
- Changer les mots de passe tous les 6 mois (session, courriel, banque, etc.)

Parlons mots de passe (2/2)

- Ne jamais stocker les mots de passe sans protection
- Éviter l'utilisation de questions secrètes (vous n'êtes pas seul·e à connaître les réponses)
- Ne pas les enregistrer dans le navigateur
- Vérifier régulièrement les fuites de données, changer les mots de passe concernés et ne plus les réutiliser (nulle part)
- Utiliser des coffres-forts sécurisés (plutôt qu'un document Word ou Excel pour les noter) : KeePassX, Bitwarden, Dashlane, NordPass ($), 1Password ($)
- Activer la double authentification quand c'est possible

Trouver un mot de passe ?

- https://pwdtest.bee-secure.lu/ (combien de temps pour cracker un mot de passe?)
- https://www.objectif-securite.ch/os_labs (crackeur de mot de passe)
- https://haveibeenpwned.com/ (ai-je été compromis·e?)

D) Que faire en cas de problème ?

- Se rappeler : **je ne suis pas coupable, mais victime !**
- Prendre quelques secondes de réflexion
- Puis-je avoir une action efficace rapidement ? (changer le mot de passe que je viens de donner, éteindre le poste compromis, déconnecter le réseau…)
- Informer les personnes concernées : responsable hiérarchique, responsable sécurité (ça permet de protéger d'autres personnes!)
- Déposer plainte
- Réinstaller le système (ça ne suffit parfois pas)