03-13 Conférence: Technologies de l'information et sécurité numérique

Cette conférence aborde l’interaction entre les technologies de l’information et le fonctionnement humain, en mettant l’accent sur la littératie numérique, la protection des données, et les arnaques basées sur des mécanismes psychosociaux. Elle explore l’impact des pannes informatiques, le vol de données, et les techniques de manipulation telles que l’ingénierie sociale. Des solutions comme le chiffrement de bout en bout, l’authentification à deux facteurs, et l’utilisation de gestionnaires de mots de passe sont discutées pour renforcer la sécurité numérique.

Points clés abordés

- Technologies de l’information et fonctionnement humain
- Arnaques basées sur des mécanismes psychosociaux
- Importance de la littératie numérique
- Impact des pannes informatiques sur les humains
- Vol d’ordinateurs et perte de données
- Conséquences psychologiques et économiques des vols
- Citoyenneté numérique et société physique
- Importance des sauvegardes de données
- Problèmes de sécurité liés aux appareils numériques
- Exemples de vols et leurs impacts

Moments forts

- → "Comprendre que la perte de données peut affecter notre santé mentale, notre réputation peut nous affecter économiquement."
- → "La protection de votre patrimoine numérique se fait aussi par des moyens physiques."
- → "La technologie peut être inquiétante, mais elle peut aussi être un facteur de soulagement et de sérénité."
- → "Tout le monde peut être vulnérable à un moment ou à un autre."
- → "Il faut développer des réflexes de vigilance émotionnelle et intellectuelle face aux manipulations."
- → "Il y a des moyens conventionnels assez simples par lesquels on peut croiser l'information."
- → "Attention aussi, dès qu'on vous demande un truc comme ça, appelez votre ami."
- → "Si vous avez un doute, partez du principe que c'est peut-être pas vrai."

Sécurité numérique et protection des données

Sécurité informatique et vulnérabilités

- L'impact des pannes informatiques va au-delà du simple système (peut toucher la sécurité physique, par exemple dans une voiture autonome)
- La perte ou le vol de données peut affecter la santé mentale, la réputation et l'aspect économique de la vie personnelle
- Importance de considérer l'ordinateur ou le smartphone comme un élément clé dans la vie au sens propre et figuré

Problèmes liés au vol et à la sauvegarde

- Cas réel : Vol d'ordinateur et tablette contenant la thèse de doctorat (version finale et corrigée), sans copie de sauvegarde
- Conséquences graves sur le plan psychologique et professionnel (perte d'années de travail, perte d'emploi)
- Autre exemple : Doctorante victime de « home jacking » dont l'ordinateur contenant sa thèse a été volé, causant une détresse émotionnelle majeure
- Importance de la sauvegarde régulière (physique et dans le cloud) et de la vérification de la fiabilité des supports de sauvegarde

Protéger ses données grâce au chiffrement

- Différenciation entre chiffrement traditionnel (où le prestataire détient la clé) et chiffrement de bout en bout (la clé est uniquement détenue par l'utilisateur)
- Exemples d'applications de messagerie sécurisées (WhatsApp, Signal, etc.)
- Nécessité d'utiliser un bon prestataire pour les sauvegardes cloud (par exemple, prestataires suisses recommandés)

Importance de la sécurité physique associative

- L'espace personnel (domicile) n'est pas infaillible face aux intrusions physiques
- Recommandation de protections physiques (comme des serrures efficaces) pour protéger les périphériques mobiles contenant des données sensibles
- La protection d'un système numérique passe aussi par la protection physique de l'environnement (exemple : vol dans un véhicule, ou protection via une bonne serrure sur la porte d'entrée)

Gestion des mots de passe et authentification

Bonnes pratiques pour les mots de passe

- Utilisation de mots de passe uniques pour chaque compte
- Comparaison avec la nécessité de sécuriser la porte d'un appartement : une "phrase de passe" peut être plus mémorable et sécurisée
- Conseils d'utiliser des gestionnaires de mots de passe (exemple : Bitwarden, OnePassword, Dashlane) pour centraliser et sécuriser les informations confidentielles
- L'authentification à deux facteurs (2FA) est recommandée pour protéger l'accès aux comptes même si le mot de passe est compromis

Risques liés au stockage non sécurisé de mots de passe

- Enregistrement dans des navigateurs ou sur papier n'offre pas une sécurité de premier ordre
- Exemples d'arnaques où des voleurs utilisent des keyloggers ou autres appareils pour enregistrer les frappes
- Importance d'utiliser des applications type Google Authenticator pour gérer la 2FA et d'éviter de synchroniser excessivement entre appareils

Sauvegarde, effacement des données et récupération

Sauvegarde

- Privilégier une sauvegarde physique et une sauvegarde cloud sécurisée avec un prestataire fiable
- Vérifier régulièrement les sauvegardes pour éviter les défaillances lors de la récupération (exemples d'erreurs de système lors du besoin urgent)

Effacement sécurisé

- Effacer des données en sachant que l'effacement conventionnel ne supprime que le repère de leur emplacement
- Utilisation de logiciels spécialisés pour un effacement complet et sécurisé afin d'empêcher leur récupération par des logiciels de récupération de données

Utilisation des outils d'intelligence artificielle (IA)

Assistance pour la cybersécurité

- Utilisation d'outils conversationnels (ChatGPT, Perplexity) pour guider, expliquer et dépanner en matière de sécurité numérique
- Possibilité de poser des questions complexes (exemple : procédures d'effacement définitif) et d'obtenir des réponses détaillées sans devoir maîtriser la technologie
- Utilisation de la recherche approfondie via ces outils pour trouver des solutions adaptées à différentes problématiques (sauvegarde, authentification forte, dépannage)

Risques humains et sociaux dans le contexte numérique

Manipulation psychologique et ingénierie sociale

- Différenciation entre les technologies de l'information et le fonctionnement humain (influence des biais cognitifs et psychosociaux)
- Exemples de fraudes téléphoniques (faux policiers, escroqueries par téléphone évoquant l'urgence pour débloquer de l'argent ou sauver un proche)
- Mécanismes exploités : détournement de l'attention, création d'un sentiment d'urgence, appel à la sympathie et à l'engagement progressif (pied dans la porte)
- Utilisation de techniques comme le phishing qui imitent visuellement des pages légitimes pour inciter l'utilisateur à fournir ses identifiants

Rôle des biais cognitifs

- Importance de la prise de distance critique et de la vigilance (exemple de la cécité attentionnelle illustrée par l'expérience des gorilles)
- Notion de "distance émotionnelle" pour éviter de se laisser manipuler par un stress ou une urgence artificiellement générée
- Nécessité de vérifier les messages et appels suspects par d'autres canaux (contacter la banque ou un proche pour confirmation par exemple)

Fraudes et arnaques basées sur le numérique

Techniques utilisées par les fraudeurs

- Spoofing téléphonique pour masquer l'identité réelle de l'appelant
- Utilisation de faux numéros d'appels et de faux emails structurés pour obtenir des informations personnelles
- Infiltration via USB ou support mobile infecté pour propager des logiciels malveillants (exemple de clé USB laissée dans un lieu public)

Exemples de fraudes spécifiques

- Cas d'arnaques par phishing envoyant des liens ressemblant à des pages de login légitimes (exemple : faux support Microsoft)
- Fraude liée à l'ingénierie sociale dans des réseaux sociaux (utilisation d'informations personnelles pour contourner la vérification d'identité)
- Techniques sophistiquées : manipulation vidéo en temps réel par IA pour simuler des rencontres et convaincre la cible de verser des fonds ou d'investir
- Arnaques reposant sur la rareté et la preuve sociale (exemple : concours frauduleux utilisant des témoignages fabriqués)

Protection par la vérification externe

- Importance de consulter des sources fiables et des avis d'experts pour valider la véracité d'un message ou d'un site internet
- Utilisation de plateformes publiques de vérification de données volées (exemple : https://haveibeenpwned.com/ sites qui comparent votre email ou mot de passe, sans exposer les données brutes)
- Nécessité de vérifier les informations d'entreprise (numéros Siren, adresses physiques réelles, etc.) pour détecter des sites frauduleux

Impact de la technologie sur la société et la perception de la réalité

Production de contenus numériques falsifiés

- Diffusion de fausses images et vidéos créées par l'intelligence artificielle (exemple : photos d'Einstein ou réécriture de l'histoire)
- Risques de confusion entre contenu réel et contenu généré, conduisant à une perte de confiance dans certaines informations médiatiques
- Effets sur la perception publique et les débats politiques, avec l'apparition de contenus manipulés (exemple : faux témoignages, fausses déclarations)

Importance de développer la capacité de discernement

- Nécessité de former l'utilisateur à adopter une distance critique face aux contenus numériques
- Encouragement à l'auto-apprentissage via des outils d'IA pour comprendre les mécanismes cachés derrière certaines arnaques ou fraudes
- Rappel que le renforcement de la vigilance (à la fois au niveau technique et psychologique) reste la meilleure protection contre les manipulations en ligne

Exemples concrets et témoignages

Expériences personnelles et retours d'expérience

- Cas d'un vol d'équipement contenant des travaux doctoraux sans sauvegarde, entraînant des conséquences professionnelles et psychologiques
- Incidents liés à des arnaques par phishing et l'utilisation de fausses pages de login (faux support Microsoft, faux appels d'agences de sécurité)
- Témoignages de difficultés liées à la configuration des outils de sauvegarde et de sécurité, et l'importance de la vigilance quotidienne

Cas de manipulation émotionnelle et financière

- Fraudes affectant des personnes vulnérables par manipulation des sentiments (exemple : sextorsion, escroqueries où la confiance est exploitée pour obtenir des virements)
- Utilisation d'IA pour simuler des rencontres authentiques et convaincre la victime d'investir ou de transférer de l'argent

- Mise en garde contre les appels à dons frauduleux et les messages qui jouent sur la peur et l'urgence pour provoquer une réaction hâtive

Aspects transversaux et recommandations pratiques

- Adopter une gestion rigoureuse des mots de passe et recourir à une authentification multifactorielle
- Mettre en place des sauvegardes redondantes et tester régulièrement leur efficacité
- Se servir des outils d'intelligence artificielle comme support d'aide pour comprendre et vérifier les contenus suspects
- Vérifier systématiquement l'authenticité des communications (emails, appels) en utilisant des canaux alternatifs et des sources officielles
- Se former aux bases techniques (lecture des en-têtes d'email, reconnaissance des URL et des sous-domaines) afin de déceler les anomalies
- Maintenir une attitude critique face aux contenus en ligne, notamment lorsqu'ils suscitent une forte réaction émotionnelle ou urgentiste

Élargissement des enjeux aux domaines physiques et sociétaux

- L'intégration de dispositifs de sécurité physique (bonne serrure, contrôle d'accès) vient compléter la protection numérique
- La protection de la vie privée doit s'étendre au monde réel (gestion des documents sensibles, déchiquetage des papiers administratifs)
- La surveillance des informations personnelles volées, via des initiatives publiques et des outils spécialisés, renforce la protection de l'identité
- Convergence entre sécurité numérique et sécurité physique permettant de voir le numérique comme une extension de la société

Conclusion synthétique des enjeux abordés

La convergence des mondes numérique et physique

L'évolution du numérique et des technologies d'information impose une vigilance constante qui doit être à la fois technique et psychologique. Nous vivons désormais dans un monde où la frontière entre espace numérique et espace physique s'estompe progressivement. Cette fusion transforme profondément la nature des risques et leurs impacts. Une panne informatique dans une voiture autonome peut mettre en danger la vie de ses occupants; le vol d'un ordinateur contenant une thèse peut détruire des années de travail et compromettre une carrière. Cette réalité nouvelle exige une reconceptualisation de notre rapport aux technologies - nos appareils électroniques ne sont plus de simples outils mais des extensions de notre patrimoine intellectuel, émotionnel et professionnel.

La dualité technique et humaine de la cybersécurité

La maîtrise des outils de sécurité (sauvegarde, chiffrement, authentification) doit impérativement s'accompagner d'une éducation aux mécanismes de manipulation sociale. L'ingénierie sociale exploite non pas des failles techniques mais notre propre fonctionnement cognitif et psychosocial. Les fraudeurs utilisent systématiquement des principes éprouvés tels que l'urgence, la sympathie, l'autorité ou la réciprocité pour contourner nos défenses rationnelles. Cette dimension humaine de la cybersécurité rappelle que même les personnes techniquement compétentes peuvent être vulnérables dans certaines circonstances, notamment lors de périodes de fragilité émotionnelle. Développer des réflexes de vigilance émotionnelle et intellectuelle devient donc aussi important que de maîtriser les outils techniques de protection.

L'intelligence artificielle : menace et solution

Le recours aux outils d'IA peut fournir une aide essentielle pour naviguer dans la complexité technologique, tout en soulignant la nécessité d'un esprit critique renforcé pour discerner le vrai du faux. L'IA représente un paradoxe dans le paysage de la cybersécurité: d'un côté, elle permet aux cybercriminels de créer des contenus trompeurs de plus en plus sophistiqués (deepfakes vidéo, images générées, textes personnalisés); de l'autre, elle offre des outils d'analyse et d'apprentissage qui peuvent démocratiser l'accès à l'expertise en sécurité. Cette dualité illustre la course permanente entre attaques et défenses qui caractérise le domaine de la cybersécurité, nécessitant une adaptation continue et une pensée critique particulièrement vigilante face aux contenus générés artificiellement.

La sécurité comme système intégré

L'intégration des mesures de sécurité sur les plans numérique et physique est essentielle pour protéger le patrimoine personnel, professionnel et émotionnel dans un monde de plus en plus interconnecté. Une approche holistique de la sécurité reconnaît

que les vulnérabilités peuvent se manifester à différents niveaux: une serrure défectueuse peut compromettre un ordinateur contenant des données sensibles; un mot de passe faible peut exposer des informations personnelles intimes. Cette vision systémique souligne que la responsabilité est partagée entre individus, organisations et institutions. Elle implique également que la formation à la sécurité numérique doit être accessible à tous et intégrée dans l'éducation fondamentale, au même titre que les autres compétences essentielles.

Une culture de résilience numérique

Développer une véritable culture de résilience numérique constitue le défi majeur de notre époque. Cette culture repose sur la compréhension des mécanismes techniques et psychologiques exploités par les cybercriminels, mais aussi sur la capacité à maintenir une distance critique face à l'information et aux sollicitations numériques. Elle implique de privilégier la vérification croisée des informations, d'accepter le doute comme posture saine, et de reconnaître que la technologie peut être à la fois source d'inquiétude et facteur de sérénité lorsqu'elle est maîtrisée. En définitive, la sécurité dans notre monde numérique n'est pas tant une destination qu'un processus continu d'apprentissage et d'adaptation, où la compréhension de notre propre fonctionnement humain devient aussi importante que la maîtrise des technologies.

Vers une éthique de la citoyenneté numérique

La notion émergente de citoyenneté numérique nous rappelle que nous évoluons désormais dans un espace commun qui génère des droits mais aussi des responsabilités. Cette dimension éthique encourage chacun à contribuer à un environnement numérique plus sûr en adoptant des pratiques responsables, en partageant ses connaissances avec son entourage, et en refusant de blâmer les victimes de cyberattaques. Elle nous invite également à préserver un équilibre sain entre connexions numériques et relations dans le monde physique, rappelant que la rencontre en personne reste un ancrage essentiel dans un monde de plus en plus virtuel. Cette éthique de la responsabilité numérique ne vise pas à créer un climat de méfiance généralisée, mais plutôt à promouvoir une utilisation consciente et réfléchie des technologies au service du bien-être individuel et collectif.