Sécurité informatique : Objectif disposer en permanence d'un ordi en parfait état de fonctionnement

Des enjeux fondamentaux :

- ✓ Elever le niveau connaissances sur les vulnérabilités et les dangers
- ✓ Sensibiliser aux comportements pour se protéger des pièges et malveillances
- ✓ Apprendre à gérer une situation critique en cas de panne ou de malveillance
- ✓ Sensibiliser aux moyens préventifs à mettre en œuvre

Défaillances physiques et logicielles – Entretien d'un ordi

- La pollution par Windows et applications
  - Windows pas mis à jour = une bombe à retardement (faille de sécurité)
  - Accumulation de fichiers inutiles (fichiers temporaires…)
  - Accumulations d'applications obsolètes et/ou inutiles
  - Disques et partitions mal gérés (programmes et données séparées)
  - Dossiers / fichiers corrompus
  - Paramétrages et optimisations insuffisants
- La pollution par l'environnement
  - Poussières, fumée, tabac, liquides de toutes sortes
  - Encrassement des composants
  - Surchauffe, vieillissement prématuré des composants
- La pollution par des intrus
  - Entrées par les réseaux, les périphériques
  - Adwares, malwares en tous genres
  - Code malveillant avec ou sans prise de contrôle
- Anticiper - entretenir – nettoyer (Cf. Tutoriel Entretenir son ordinateur)
  - Mettre à jour Windows 10 (75 vulnérabilités corrigées en mars 2018)
  - Paramétrer / optimiser un ordi
  - Définir un Plan de maintenance et l'appliquer
  - Diagnostic – vérifier l'état de fonctionnement
  - Le nettoyage physique
  - Le nettoyage avec les outils de Windows
  - L'entretien avec d'autres outils reconnus fiables

Les Vulnérabilité et les Dangers du Net

Les vulnérabilités

- Atteinte aux personnes
  - Vol d'identité
  - Attaques calomnieuses
  - Désinformation à grande échelle (Fakes News), projet de loi annoncé
  - Diffamation et dénigrement, atteinte à la vie privée
  - Atteinte à l'e-réputation (réseaux sociaux)
  - Viol et agressions sexuelles via le net
- Dommage aux biens
  - Piratage d'ordinateur ou téléphone,
  - Destruction ou vol de données,
  - Contrefaçon et escroqueries en tout genre
  - Prise de contrôle sur les objets connectés
- Cyberattaques
  - Prise de contrôle sur des équipements sensibles ((hôpitaux, trains…)
  - Prise de contrôle sur des sites stratégiques (armée, nucléaire,…)
  - Attaques de régions ou pays entiers (cyberguerre)
  - L'ONU et la prochaine guerre mondiale Ciber

Les Dangers du net

- **Les dangers du net via le Web**
  - L'explosion des réseaux sociaux et du mobile dans le monde
  - L'explosion du nombre de sites frauduleux
  - Les enregistreurs de frappe au clavier (keylogger)
  - Désactiver l'enregistreur de Windows 10
  - Le marché noir des comptes bancaires volés (ordis zombis)
  - Le vol des mots de passe dans les navigateurs (Firefox,…)
  - Les pop-ups, l'envahissement de la publicité
  - Le vol des données personnelles et le profilage (Big Data)
  - Les adwares, Les virus et malwares, les intrusions
  - Les pièges et dangers du net (vidéo complète)

- **Les dangers via la messagerie**
  - Le Spam
  - Le phishing
  - Les ransomwares
- **Les dégâts collatéraux**
  - La dépendance
  - La pornographie,
  - La désinformation,
  - Les prédateurs sur le Net

Parmi les plus grands types de fraudes répertoriés, la Cybercriminalité apparaît comme le risque majeur à l'avenir en France : 73% des dirigeants français anticipent une importante augmentation du risque de cybercriminalité. La France est le 9ème pays au monde où la cybercriminalité est la plus active. L'Etat en appelle les télécoms à la rescousse.

La Mécanique d'infection

- La Publicité les pop-up
  - Qui a inventé les fenêtres pop-up ? (et surtout pourquoi ?)
    - Web des années 90 : les bannières publicitaires
    - Les sites remplacent les bannières par des pop-up
    - Les pop-up contiennent des Adwares : scripts publicitaires
  - Les Adwares polluent les navigateurs et les ordis
    - Les Adwares s'accompagnent de scripts malveillants : malwares
- Adwares / Malwares attendent vos clics de souris
  - Via les sites web frauduleux spécialistes en bicoints et cryptomonnaies
  - Via les Crypto-ver pour propager les ransomwares sur le web
  - Via la messagerie encore plus frauduleuse en 2018
  - Via l'installation de logiciels gratuits
  - Via tout type d'application existante sur un ordi vulnérable ou infecté

- Les Liens et les redirections sur internet
  - Les redirections frauduleuses
  - Le clic qui tue, je réfléchis puis je clique (et non l'inverse)
  - Les yeux rivés sur l'URL (nom de domaine)

La Protection « logiciels »

- Corriger les failles de sécurité
  - Un Windows constamment mis à jour (Tuto sur Infoweb17fr)
    - Les Patchs Tuesday
    - Et autres mises à jour de produits Microsoft
  - Toutes les applications à jour, supprimer les obsolètes
- Installer les outils indispensables
  - Un anti-virus : Avast ou autre avec filtre ransomwares
  - Des bloqueurs de Pub type Adblock
    - Ccleaner, Adwcleaner,
    - Malwarebytes, etc…
  - Eviter les assistants nettoyeurs/optimiseurs type Glary Utilities
- Bien les paramétrer ses navigateurs et outils de messagerie
  - Comprendre les méthodes de messagerie
  - Activer l'anti hameçonnage dans les navigateurs
  - Gérer ses mots de passe dans Firefox
  - Paramétrer ses outils de messagerie
    - Orange, SFR, …

La Solution est dans son comportement sur le Net

- Apprentissage minimal (Astuces)
  - Maîtriser l'outil informatique, le web, la messagerie électronique
  - De nombreux sites web pour apprendre (y c. aux enfants)
  - Revues et organismes divers : cybermalveillance.gouv.fr
- Maitriser ses réflexes avant tout : je réfléchis puis je clique (non l'inverse)
  - Internet est un espace public (prudence d'y raconter sa vie personnelle)
  - Pas de clic sur la pub des pages web
  - Pas de clic sur un lien texte ou image d'un mail
  - Ne pas ouvrir un mail suspect, sécuriser ses données personnelles
  - Etre capable d'échapper au phishing
  - Vérifier l'adresse exacte de l'émetteur du mail
  - Ne pas se connecter à partir du mail pour fournir identifiant et mot de passe
  - Résister aux offres alléchantes, déceler les arnaques courantes
  - Ne pas être le pigeon du Net, l'url https:// vous vérifiez ?
  - Situation critique : fermer une tâche avec le gestionnaire de tâches

- Avoir un Plan catastrophe pour tout rétablir en cas d'incident (Backup)
- Avoir au moins deux adresses mail (une spécifique pour le Net)
- Changer ses mots de passe plus solides plus régulièrement
- Bloquer les mails indésirables etc… Continuer à suivre de près ce dossier !

En guise de conclusion

L'objectif de pouvoir disposer de ses outils informatiques en parfait état de marche à tout moment peut sembler utopique voire totalement illusoire.

En cause, la vulnérabilité des matériels et logiciels, la méconnaissance des utilisateurs, le haut niveau d'expertise des hackers, les retards pris par les autorités pour combattre la cybercriminalité, l'insuffisance de prise en compte de la sécurité dans la fabrication des objets connectés, et surtout le maillon faible qu'est l'interface chaise-clavier.

Numérisation et mondialisation expliquent la mutation profonde de notre nouveau monde cybernétique et impactent directement la manière de notre vivre ensemble.

Tout se passe comme si depuis des années, les campagnes de sensibilisation restaient lettres mortes, pire, les émetteurs privés ou publics de ces consignes avouent ne pas se les appliquer à eux-mêmes. Résultats : 2017 le début des années records cyber-catastrophes.

Les hackers (publics ou privés) règnent en maître du monde, la question n'est plus de savoir si une catastrophe d'envergure est possible mais où et quand elle va se déclencher.

Réveil tardif et douloureux, les Etats en sont réduit à avouer leur incapacité à trouver des parades efficaces, l'heure est jugée grave face aux cyberguerres impitoyables annoncées.

Avoir conscience de la gravité de la situation, sortir de la méconnaissance informatique et numérique de notre nouveau monde connecté, adapter sans cesse son comportement d'utilisateurs d'ordi, tablettes, smartphones et tout autre objet connecté avec toute la vigilance voire la méfiance qui s'impose, sont autant de démarches impératives et incontournables à tous les niveaux de notre pratique au quotidien.

Bonne vigilance et bonne réflexion à tous, merci de votre attention.

Annexes :

Quelques documents sur la sécurité informatique

- Entretenir son ordinateur : matériels et logiciels
- Configurer son nouvel ordinateur : partir du bon pied avec les outils de base
- Paramétrer / Optimiser un PC Windows 10
- Les Cyberattaques et prises de contrôle par les hackers : JT de 20H le 11 mars 2018
- Les Cyberattaques mondiales pourquoi c'est grave ? : Emission C dans l'air 2017
- Renault, hôpitaux, gares, … touchés par les cyber-pirates informatique
- Piratage informatique : Un Pearl Harbour informatique est tout à fait faisable
- L'arrivée des Crypto-ver sur le web
- Le Guide d'hygiène informatique 2013 cet opuscule si vite enterré
- Les pièges et les dangers du net : une petite vidéo de sensibilisation
- Le Guide sur les ransomwares et la façon de vous en protéger
- Le phishing ou hameçonnage : des exemples en images
- Les faux e-mails Amazon plus vrais que nature
- Le piratage de votre carnet d'adresses ou votre messagerie
- La cybercriminalité est devenue la 1ère fraude en France
- La Cybercriminalité : un phénomène en explosion
- La Cybercriminalité menace la planète : fraude de 600 millions de dollars en 2017
- Quelques liens web sur la sécurité informatique en 2018
- Un diaporama sur la sécurité informatique
- Un portail de la sécurité informatique avec Wikipédia
- L'actualité de la sécurité informatique suivie par Le Monde
- La sécurité informatique en vidéos sur YouTube

oOo