Découverte du monde numérique

Session 6

Jean-Marc Joncour

27 Avril 2023

JIMAJIN

Les Thématiques

1. *Historique de l'informatique, Les matériels (Hardware)*
2. *Les systèmes d'exploitations (Operating System ou OS) et Windows 10 en particulier*
3. *Les navigateurs Internet : Edge, Chrome, Firefox , Les unités informatiques : kilo, mega, giga, tera,*
4. *La messagerie électronique (emails)*
5. *Les logiciels (Software) : Intro, traitement de texte Word, LibreOffice Writer*
6. La Cyber Sécurité : Anti-virus, Phishing, gestion des mots de passe, les bonnes pratiques, les arnaques
7. Les tableurs Excel, LibreOffice Calc
8. Les logiciels graphiques Powerpoint , Retouche photos avec GIMP
9. Le réseau : La box, Ethernet, Wifi, Bluetooth , La connectique et les câbles (USB, HDMI,...)
10. Les logiciels de collaboration : Teams, Zoom
11. L'impression et la numérisation de documents ou de photos, les fichiers PDF
12. L'intelligence artificielle, Les réseaux sociaux et les sites Internet : Google, Facebook, Youtube et les sites officiels (Impôts, Retraite, Ameli, FranceConnect...)
13. Les Smartphones et les applications mobiles
14. Les crypto-monnaies, Le Metavers, L'impression 3D, La Domotique,
15. Le Darknet, Les sauvegardes, la prise de contrôle à distance. La virtualisation, La programmation,
16. L'examen

Architecture e-mail

jmjoncour@gmail.com → GMAIL est le prestataire → La boite aux lettres est dans le cloud Internet

Les ordinateurs ou smartphones peuvent consulter les e-mails

Smartphone

- Application comme Outlook ou GMAIL
- Accès par un navigateur (webmail)

Ordinateur

- Application comme Outlook
- Accès par un navigateur (webmail)

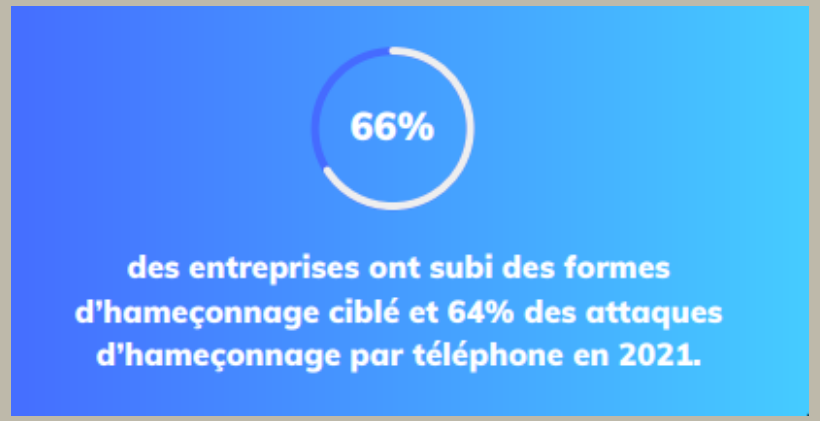
Cela vous dit quelque chose ?

Jimajin

La Cybersécurité

La cybersécurité consiste à protéger les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes. On l'appelle également sécurité informatique ou sécurité des systèmes d'information.

- La **sécurité réseaux** consiste à protéger le réseau informatique contre les intrus, des attaques ciblées ou des malwares..
- La **sécurité des applications** vise à protéger les logiciels et les appareils contre les menaces.
- La **sécurité des informations** veille à garantir l'intégrité et la confidentialité des données.
- La **sécurité opérationnelle** comprend les processus et les décisions liés au traitement et à la protection des données.
- **La reprise après sinistre et la continuité des opérations** spécifient la manière dont une entreprise répond à un incident de cybersécurité
- **La formation des utilisateurs finaux** porte sur le facteur le plus imprévisible : les personnes. Tout le monde peut accidentellement introduire un virus dans un système habituellement sécurisé en ne respectant pas les bonnes pratiques de sécurité.



Le Phishing ou hameçonnage

- L’hameçonnage ou phishing est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité.
- La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, numéro ou photocopie de la carte d'identité, date de naissance, etc.
- Une copie exacte d'un site internet est réalisée dans l'optique de faire croire à la victime qu'elle se trouve sur le site internet officiel où elle pensait se connecter.
- La victime va ainsi saisir ses codes personnels qui seront récupérés par celui qui a créé le faux site.

Il faut toujours utiliser les favoris pour accéder à un site bancaire ou un site de l’administration française.

L’arnaque au président

L’arnaque au président connait régulièrement des variantes, l’une d’elles apparue il y a quelques mois est réalisée à grande échelle auprès des sociétés françaises.

- L’arnaque au président consiste pour le fraudeur à contacter une entreprise cible, en se faisant passer pour le président de la société mère ou du groupe.
- Le contact se fait par courriel ou par téléphone. Après quelques échanges destinés à instaurer la confiance, le fraudeur demande que soit réalisé un virement international non planifié, au caractère urgent et confidentiel.
- La société sollicitée s'exécute, après avoir reçu les références du compte étranger à créditer.

Les virus informatiques

- Un virus informatique est un automate logiciel autoréplicatif.
- Certains sont inoffensifs, d'autres contiennent du code malveillant (ce qui entraine le classement du logiciel comme logiciel malveillant).
- Un virus informatique est conçu pour se propager sur d'autres ordinateurs en s'insérant dans des logiciels légitimes, appelés « hôtes » à la manière d'un virus biologique.
- Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté.
- Un virus se répand par tout moyen d'échange de données numériques, comme les réseaux informatiques ou les périphériques de stockage externes (clés USB, disques durs, etc.).

Les ransomwares (rançongiciels)

Les ransomwares sont des logiciels d'extorsion qui peuvent verrouiller votre ordinateur et demander une rançon en échange du déverrouillage de celui-ci.

- Mettre régulièrement à jour votre logiciel et votre système d'exploitation
- Veillez à mettre à jour vos logiciels et votre système d'exploitation. Il s'agit d'une étape de protection essentielle contre les ransomwares.
- Ne pas cliquer sur les liens suspects
- Ne jamais ouvrir les pièces jointes d'emails provenant d'expéditeurs non approuvés
- N'effectuer aucun téléchargement depuis les sites Web non fiables
- Éviter d'utiliser des supports USB inconnus

Sécurisation du compte email

- Il est extrêmement important d'avoir un **mot de passe solide** pour protéger sa boite mail.
  - Un mot de passe solide c'est plus de 8 caractères incluant des majuscules, des minuscules, des chiffres et des caractères spéciaux.
  - Exemples : LpdlrK_007-$, Fpp-Ledbd-Pdcs_97 , Lacpa#85
  - Les très mauvais mots de passe : 123456, porsche, qwerty, cameron, superman, tomcat , ferrari, motdepasse, password1234
  - Le mot de passe choisi ne doit pas être utilisé pour d'autres sites.
- Beaucoup de services utilisent l 'email pour s'identifier et renvoient un lien pour changer son mot de passe
- Attention à l'usurpation numérique !
- La recommandation est d'utiliser un gestionnaire de mots de passe (Lastpass, 1Password, **Dashlane**, Keepass, Cloud Pass, ...)

Les anti-virus

- Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants
- Ces derniers se basent sur l'exploitation de failles de sécurité,
- mais il peut également s'agir de logiciels modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur (le plus souvent ceux du système d'exploitation).
- Les anti-virus les plus connus : Microsoft Defender, Avast, McAfee, AVTotal, Panda, Norton, Avira ,

Les gestionnaires de mots de passe

- Outil permettant de stocker les mots de passe dans un coffre-fort sécurisé.
- Exemples : 1Password, LastPass, **Dashlane**, Keepass
- 1 mot de passe Maître à conserver

Authentification Multi-Facteurs

Authentification Multi-Facteurs

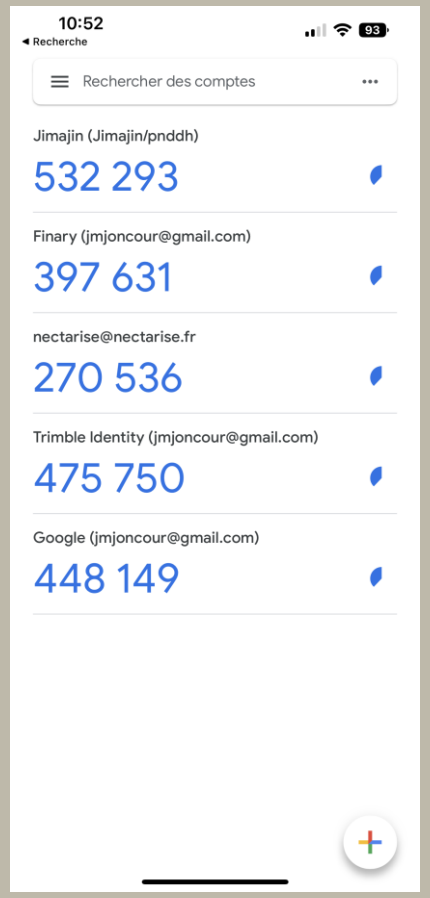
Un deuxième niveau de sécurité

Authentification Multi-Facteurs

- L'authentification multifacteur permet de renforcer la sécurité de l'accès à vos comptes grâce à l'ajout d'un ou de plusieurs facteurs d'authentification.

- Vous la trouverez parfois désignée par le sigle « 2FA » (pour l'anglais « 2-factor authentication », authentification à deux facteurs), par « validation en deux étapes » ou encore « MFA » (pour l'anglais « multi-factor authentication », l'authentification multifacteur).
- Méthodes:
  - SMS
  - Application sur Smartphone

Applications d'Authentification sur SmartPhones



Google Authenticator

Microsoft Authenticator

Des cas concrets …

- Exemples d'emails frauduleux avec les spams de Gmail ou jm_joncour@hotmail.com

- Les évènements récents : voir les liens

Exemples de smishing

Le smishing est l'équivalent du phishing email pour les SMS.
Il s'agit de messages SMS envoyés aux détenteurs de smartphones dans le but de leur dérober des données personnelles ou bancaires.

Techniques avancées

Une simple image peut-elle être dangereuse pour votre ordinateur ? Oui, répondent les chercheurs en sécurité de Symantec, une entreprise connue pour l'antivirus Norton. Dans un rapport publié sur le site web de Symantec, ils dénoncent les agissements d'un groupe de hackers nommé Witchetty . Ce groupe utilise la technique de la stéganographie, qui consiste à cacher des données dans une image. Ainsi, un logo de Windows semblable à celui présenté ici a dissimulé un programme malveillant

Les bonnes pratiques

- Protégez vos accès avec des mots de passe solides
- Utilisez un gestionnaire de mots de passe
- Installez/configurez un antivirus
- Activez la double authentification (multi-facteurs)
- Sauvegardez vos données importantes régulièrement
- Téléchargez les applications uniquement sur les sites officiels
- Méfiez-vous des messages inattendus même de vos amis
- Évitez les réseaux WiFi publics ou inconnus
- Séparez vos usages personnels et professionnels
- Mettez régulièrement à jour les versions de vos applications

Les sauvegardes

- La règle est d'avoir ses données importantes (photos, lettres, documents, etc) stockées sur au moins 2 unités de stockage différentes (disque, disque externe, cloud)
- Un disque dur n'est pas fiable
- Un portable peut se faire voler.
- Un virus peut supprimer tous les fichiers
- Régulièrement, une sauvegarde doit être effectuée.

2ième disque dur

Clé USB

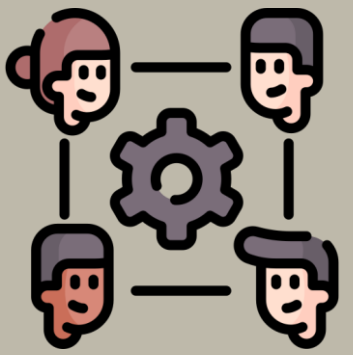
Disque externe

NAS

Cloud

Des questions ?

Atelier Travaux Pratiques



- Ouvrir le navigateur Edge en plein écran
- Si vous n'avez pas cette adresse dans vos favoris, taper l'adresse suivante dans la barre d'adresses
  - https://tinyurl.com/atelier-jimajin
- Vous devez être redirigé sur :
  - https://www.jimajin.fr/formations/atelier/
- Sélectionner la session 6
- Suivez ensuite les instructions …
- L'apéro c'est après…