SECURITE SUR INTERNET – ETRE ACTEUR

Alain JACQ
Décembre 2023

SOMMAIRE

Introduction

Notre Monde Global est Digital.

Le numérique se développe dans les secteurs économiques :

- Santé comme le Social et le monde Associatif,
- Le Commerce et les Echanges,
- L'Industrie Manufacturière,
- L' Art, la Culture et le Divertissement,

Partout

- Dans l'espace et le ciel,
- Sur la terre, à la maison, à la ville comme à la campagne,
- Dans l'Univers réel comme dans le Métaverse.

jobstory

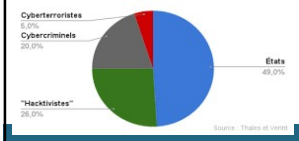
- Expertise IT un peu plus 30 ans
  - RUN et BUILD,
  - « Épicurieux » vos métiers ma passion,
  - Chargé de Mission au CMAF ➔ DRCC IT.
- Objectifs
  - Sensibilisation à la sécurité internet,
    - Environnement professionnel et personnel,
  - Cybersécurité :
    - Je ne suis pas un expert,
  - Cette présentation pour vous donner les clés,
  - Une proposition : Être Acteurs de votre Sécurité/Internet.

ENVIRONNEMENT

5

Contexte international :

Profil des cyberattaquants



- Internet :
  - Conflit russo-ukrainien,
  - Terrorisme,
  - Espionnage,
  - Cybercriminalité protéiforme,
  - Réseaux sociaux.
- Internet un Outil incroyable :
  - Muti-culturelle,
  - La Liberté & le Far west,
  - Outil de communication et de partage,
  - Education ➔ acquérir & partager les connaissances,
  - Ouverture au monde et rapprochement des cultures,
  - Réseaux sociaux,
  - Aide au Quotidien.

jobstory

CONTEXTE NATIONAL ET INTERNATIONAL

6

Selon ANSSI les menaces

- **La déstabilisation**,
  - Saturation ou déni de service pour saturer et rendre indisponible un site web. Souvent l'œuvre d'hacktivistes pour des motifs déontologiques ou des geeks pour des défis techniques,
  - Défiguration ou dénaturation de l'image pour porter atteinte à la réputation,
  - Exfiltration de données soit pour communiquer des informations confidentielles soit pour rançonnage.
- **L'espionnage,**
  - Vise essentiellement la sphère économique et les services gouvernementaux pour porter atteinte aux intérêts d'un pays, (les ennemis comme les amis
  - Hameçonnage ciblé pour atteindre des réseaux vulnérables (ex de organisations sectorielles, syndicats).
- **Le sabotage,**
  - Nuire aux Opérateurs d'Importance Vitale (Transport Energie, Télécom, Banque) pour provoque le chaos.

Les techniques d'action sont nombreuses et les profils des auteurs sont éclectiques, depuis l'individu isolé, aux hacktivistes, en passant par les organisations criminelles et des services gouvernementaux.

jobstory

Vocabulaire & Panorama & Quiz Arnaques

jobstory

VOCABULAIRE

Quiz ?

- Spam ou Pourriel → Tout courrier électronique non sollicité. Ce type de courrier inonde simultanément un grand nombre d'adresses électroniques
- Phishing, Hameçonnage, Filoutage → Vol d'identités ou d'informations confidentielles (code d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un acteur malveillant pour vous convaincre de communiquer des infos confidentielles
- Spearphishing, Hameçonnage ciblé → Basée sur usurpation d'identité . Classée dans l'ingénierie sociale forte qui lie l'objet du msg à l'activité de la personne ou de l'entreprise ciblée/ Fraude au président
- Quishing → Contraction de QR Phishing

jobstory

VOCABULAIRE

9

Quiz ?

Mail Bombing

Envoi massif de courriels à un destinataire pour saturer ou asphyxier le service de messagerie

Mail Harvesting ou Moisson de courriels

Parcourir l'internet (pages, blog, groupes discussions) afin de récupérer des emails pour des intentions malveillantes

jobstory

VOCABULAIRE

10

Quiz ?

Malicious Sotfware, Malware, Spyware

Tout programme développé dans le but de nuire à ou au moyen d'un système d'info ou d'un réseau … Les virus ou vers sont les codes malveillants les plus connus. Le Spyware ou Espiogiciel est un logiciel qui collecte et transmet à des tiers des info sur l'environnement sur lequel il est installé à l'insu du propriétaire

Adress munging, Adress Spoofing

Usurpation d'adresses mail/collecte pour diffuser des canulars, du code malicieux afin de capturer des DCP.

Ransomware ou Rançongiciel

Extorsion imposée par un code malveillant sur le système d'un utilisateur ou d'une organisation. Contraction de Rançon et Logiciel → objectif obtenir une rançon

jobstory

VOCABULAIRE

11

Quiz ?

Denial of Sercice, DoS/DDoS

Déni de service : Action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un service en le sur sollicitant. Si l'action provient de plusieurs sources Déni de Service Distribué

DNS pharming

Clonage de serveur DNS : activité d'usurpation d'un nom de domaine internet afin que le flux soit redirigé vers une adresse internet illégitime.

jobstory

ARNAQUES

12

Cybermalveillance.gouv.fr : Internet et Téléphone

- Arnaque au chantage à l'ordinateur/webcam prétendus piratées,
- Arnaque au Compte Personnel de Formation (CPF),
- Arnaque au proche en situation d'urgence,
- Arnaque à la fausse commande ou Arnaque à la commande,
- Arnaque téléphonique (*pingcall* en anglais),
- Cyberharcèlement,
- Escroquerie sentimentale,
- Escroquerie au placement financier,
- Fausses offres d'emploi créées par des fraudeurs,
- Fraude au faux conseiller bancaire,
- Hameçonnage à la carte Vitale,
- Piratage d'un objet connecté,
- Piratage d'un système informatique – Particuliers & Professionnels,
- Piratage de compte en ligne et Piratage compte bancaire,
- Piratage de la téléphonie fixe,
- Sextorsion (chantage à la webcam ciblé),
- Usurpation d'identité/numéro téléphone,
- Virus,
- Vol identité ou Vol de CB. Et beaucoup d'autre..

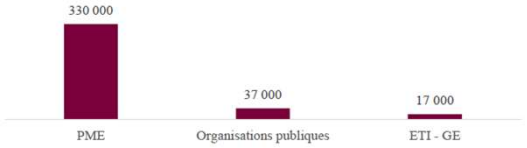
jobstory

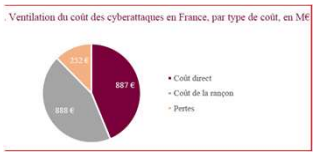
PANORAMA DE LA CYBERMENACE

13

- Attaquants améliorent leur outillage en combinant les attaques
  - Rançongiciel, ciblage des équipements périphériques, destruction de données (wipers)
- Le Gain financier, l'espionnage et la déstabilisation sont les objectifs principaux des attaquants
- Les Mêmes faiblesses exploitées
  - Vulnérabilités exploitées alors que les corrections existent,
  - Les nouvelles technologies augmentent la surface d'attaque,
    - L'externalisation de services IT dans le Cloud Computing,
  - L'opportunité offerte par les divulgations de DCP (Hameçonnage, vol de mots de passe)
- Etude cabinet Astères (CRiP)
  - Les Cyberattaques réussies ont couté en France 2Mds€ en 2022,
    - Coûts dire
    - Rançons 8
    - Perte Expl
    - 385000 at
    - Une organ

Graphique 3. Ventilation de cyberattaques réussies en 2022 entre les entreprises et les organisations publiques





jobstory

Astuces & Adresses Utiles

jobstory

CONSEILS / ALERTES

15

Service public d'alerte ou de plainte

- Moteur de recherche
  - Rechercher mots clés THESEE service Public ou PHAROS
  - Adresse : https://www.masecurite.interieur.gouv.fr/
    - *Je suis victime,*
    - *Je signale,*
    - *Je m'informe.*
- THESEE plainte /arnaque,
- PHAROS signalement de contenu illicite ou haineux,
- Litiges e-commerce
  - En France https://www.mediateurfevad.fr/ ou vos droits https://service-public.fr/particuliers
  - UE https://ec.europa.eu/consumers/odr/main
  - Reste du Monde https://www.econsumer.gov

CAPSULES VIDEO

16

Sensibilisation source Caisse d'Épargne

5 capsules vidéo de la Caisse D'Epargne

Video CE 1

Vidéo CE 2

Vidéo CE 3

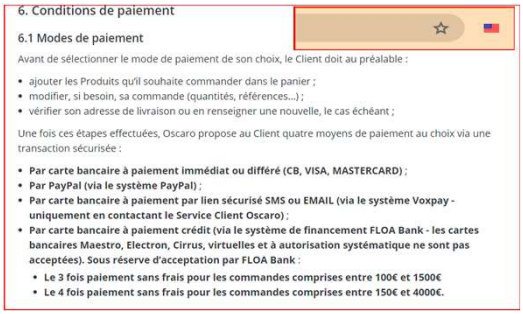
Video CE 4

Vidéo CE 5

RECOMMANDATIONS BERCY

- Choisir une double sécurité avec votre Banque code SMS en plus du code cryptogramme visuel,
- Attention aux offres alléchantes tout ce qui brille n'est pas d'OR,
- Carte bleue virtuelle ou e-carte BLEUE,
- Ne jamais enregistrer vos coordonnées bancaires sur les sites,
- Attention aux réseaux wifi publics non sécurisés mal chiffrés, des pirates peuvent l'avoir pris en mains pour capturer vos DCP,
- Assurer votre sécurité globale :
  - Matériel à jour (logiciels),
  - Antivirus à jour, analyse régulière (sur ordinateur et smartphone),
  - Consulter vos comptes bancaires régulièrement pour vous assurer qu'aucune transaction irrégulière,
  - Avoir des mots de passe solides et différents selon les sites,
  - Utiliser votre messagerie en sécurité,
- Prévenir votre banque en cas d'incident.

MES PREFERENCES



6. Conditions de paiement

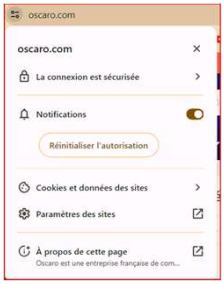
6.1 Modes de paiement

Avant de sélectionner le mode de paiement de son choix, le Client doit au préalable :

- ajouter les Produits qu'il souhaite commander dans le panier ;
- modifier, si besoin, sa commande (quantités, références...) ;
- vérifier son adresse de livraison ou en renseigner une nouvelle, le cas échéant ;

Une fois ces étapes effectuées, Oscaro propose au Client quatre moyens de paiement au choix via une transaction sécurisée :

- **Par carte bancaire à paiement immédiat ou différé (CB, VISA, MASTERCARD)** ;
- **Par PayPal (via le système PayPal)** ;
- **Par carte bancaire à paiement par lien sécurisé SMS ou EMAIL (via le système Voxpay - uniquement en contactant le Service Client Oscaro)** ;
- **Par carte bancaire à paiement crédit (via le système de financement FLOA Bank - les cartes bancaires Maestro, Electron, Cirrus, virtuelles et à autorisation systématique ne sont pas acceptées). Sous réserve d'acceptation par FLOA Bank** :
  - **Le 3 fois paiement sans frais pour les commandes comprises entre 100€ et 1500€**
  - **Le 4 fois paiement sans frais pour les commandes comprises entre 150€ et 4000€.**



- Lire des CGV et ou CGU mode de paiement
- Carte bleue virtuelle ou e-carte BLEUE,
- Vérifier que la page est sécurisée (HTTPS://) jusqu'au paiement
- et la localisation du site
- Attention aux offres alléchantes tout ce qui brille n'est pas d'OR,
- Ne pas enregistrer de coordonnées bancaires sur internet,
- Attention aux réseaux wifi publics non sécurisés mal chiffrés, des pirates peuvent l'avoir pris en mains pour capturer vos DCP,
- Enregistrer les sites dans vos favoris
- Cliquer sans modération mais toujours avec précaution
- Effacer régulièrement vos historiques de navigation/🍪
- Mettre à niveau votre navigateur porte d'entrée sur internet
- N'oublier surtout pas l'adage « Quand c'est gratuit c'est qui le produit ? »

Questions/Réponses

jobstory