Certification Tosa

By :
ANIASSS - RoBING
Mariah - Gregan

Réseau sans fil

Surexposition des données pour les nomades

Hameçonnage

Réseau Sans fil

Risques

Wifi Bluetooth sécurisé

VPN

Réseau sans fil - risques

75% des wifi public sont vulnérables

Les pirates ont accès à ce réseau pour y intercepter le trafic réseau (données personnelles) en se positionnant entre le point d'accès et la cible

Les risques communs :

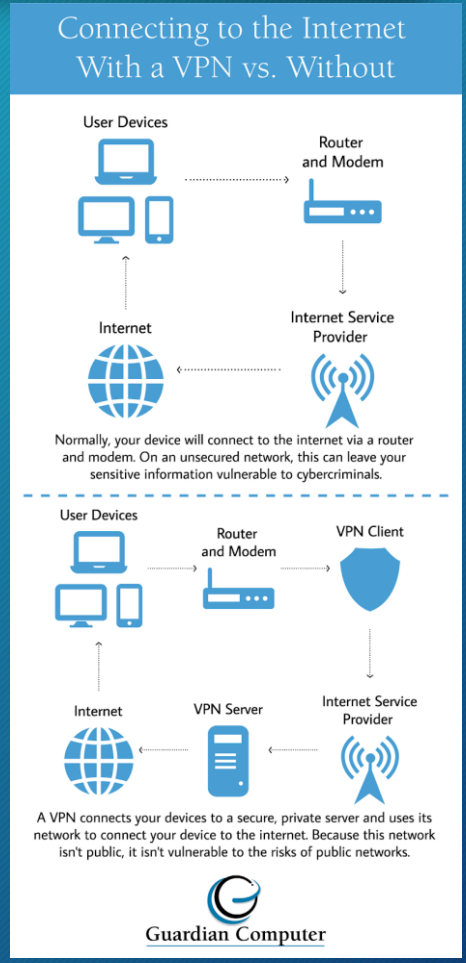
- Wifi sans aucune identification
- L'erreur humaine
- Vulnérabilités logicielles
- Connexion Bluetooth

Réseau sans fil – toujours sur du sécurisé !

1. Renommer les réseaux périodiquement avec des noms obscurs
2. Masquer le réseau pour éviter qu'il soit repris dans la liste
3. Utiliser le chiffrement le + avancé possible
4. Désactiver le partage
5. Désactiver le wifi si aucun besoin
6. Utiliser les connexions SSL pour chiffrer le trafic de bout en bout - HTTPS

Réseau sans fil – VPN Wifi Publics

- Capacité de chiffrer toutes les données qui transitent en créant un tunnel sécurisé
  entre le client en accès nomade et le serveur VPN.
- Grâce à des mécanismes robustes de chiffrement, d'authentification et d'intégrité
- Utilisation du protocole IPsec plutôt que TLS pour le tunnel VPN

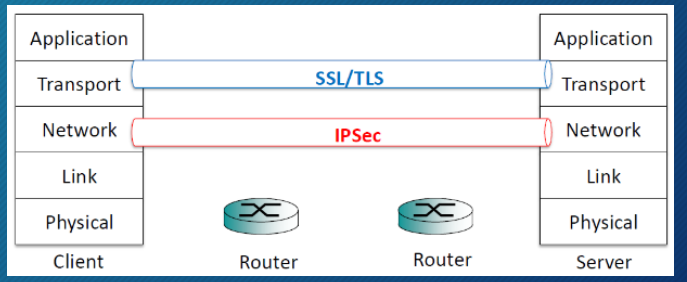


Réseau sans fil – VPN IPSec vs TLS

Utilisation du protocole IPSec plutôt que TLS pour le tunnel VPN car :

- La surface d'attaque d'IPsec + réduite & Les opérations de sécurité critiques sont dans un environnement cloisonné
- Les mécanismes de choix initial des algorithmes entre le client et le serveur sont + robustes
- la majorité des vulnérabilités récentes concerne les implémentations des protocoles SSL et TLS *(POODLE, BEAST, CRIME, FREAK, Heartbleed, etc.)*.

De manière générale, pour TLS il s'agit de mauvaises implémentations développées dans des langages qui n'apportent pas toujours un niveau de sécurité satisfaisant.



Surexposition des données pour les nomades

Nomadisme Numérique

Préconisations Avant, Pendant, Après

Surexposition des données – Nomadisme numérique

Toute forme d'utilisation des technologies de l'information permettant à un utilisateur d'accéder au SI de son entité d'appartenance ou d'emploi **depuis des lieux distants n'étant pas maîtrisés par l'entité**.

Risques exacerbés :

- Perte / vol de matériel
- la compromission du matériel
- la compromission des informations
- l'accès illégitime au SI de l'entité (et donc la compromission de celui-ci)
- l'interception voire altération des informations (perte de confidentialité et/ou d'intégrité)

Surexposition des données – Préconisations Avant

- SENSIBILISATION DES UTILISATEURS ✓
- EVITER LE TRANSPORT DE DONNÉES SUPERFLUES ✓
- S'INFORMER SUR LA LÉGISLATION DU PAYS DE DESTINATION ✓
- SAUVEGARDER LES DONNÉES EMPORTÉES ✓
- CHIFFRER LES DONNÉES EMPORTÉES ✓

Utiliser comme outil de sauvegarde ou de synchronisation les services cloud installés par défaut sur un appareil sans analyse approfondie de leurs conditions d'utilisation et des engagements de sécurité pris par les fournisseurs de ces services.

Surexposition des données – Préconisations Pendant

DISCRÉTION

- Filtre discrétion
- Evaluer la communication
- Réseaux sociaux

SURVEILLANCE DE VOS DOCUMENTS / MATÉRIELS

- Verrouillage session & auto activé
- Enveloppes inviolables
- Câble anti-vol, …
- Protection contre le vol

RÉSEAUX / MATÉRIELS / LOGICIELS MAÎTRISÉ

- VPN + Auth Forte
- Moyen professionnel (Mail, Matériel, …)
- Prestataire fiable (ProtonMail par ex.)
- Plusieurs adresses mail (personnel <> pro)
- Désactiver Wifi / Bluetooth

INFORMER EN CAS DE PERTE OU VOL

- Votre responsable de Sécurité
- Déposer plainte
- Mesures pour protéger des connexions malveillantes

Wifi publics (dernier recours)
Laisser des clients / fournisseurs / Autres tiers se connecter sur votre réseau

Cui Cui

Surexposition des données – Préconisations Après

RENOUVELER LES MOTS DE PASSE

- Authentification Forte
- Mots de passe différents
- Surtout en cas de doute

VÉRIFIER LES ÉQUIPEMENTS PAR VOTRE RESPONSABLE DE SÉCURITÉ

- Effacer les historiques
- Les Clés USB offertes :D

Utiliser ou continuer d'utiliser un matériel qui aurait :
été saisi par la « Police », déposé à des portiques d'aéroport, accueil d'entreprise

En cas de législation différente concernant le VPN , méthodes de chiffrement, …

Hameçonnage

Définition

Fonctionnement

Différentes formes

Se protéger

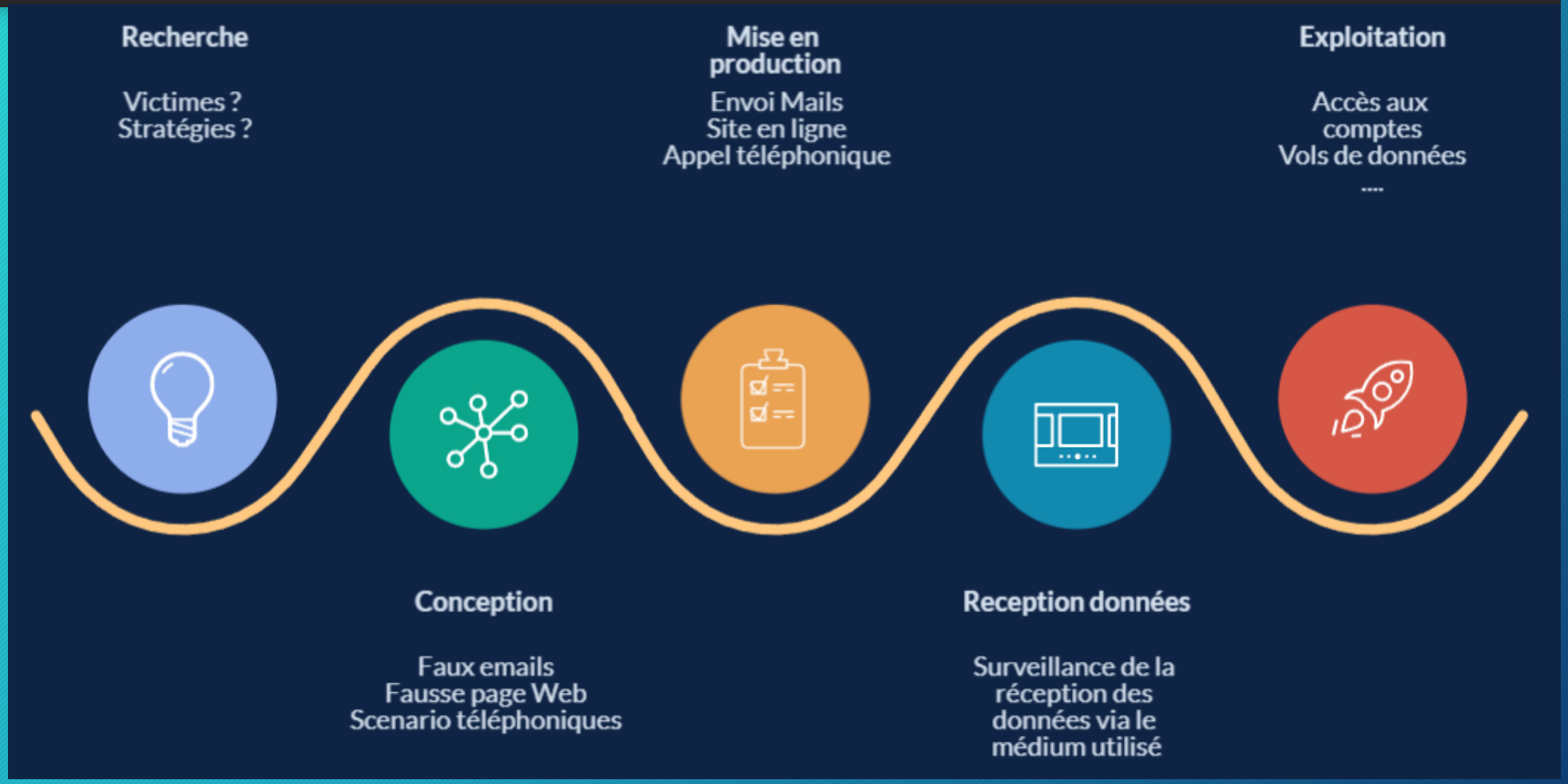
Hameçonnage - Définition

Cybercriminel prétendant être une organisation légitime pour tenter d'obtenir des données confidentielles :

- Numéro carte bancaire
- Noms d'utilisateurs
- Mot de passe
- Accès comptes importants

- Usurpation d'identité
- Pertes financières
- Vol de données

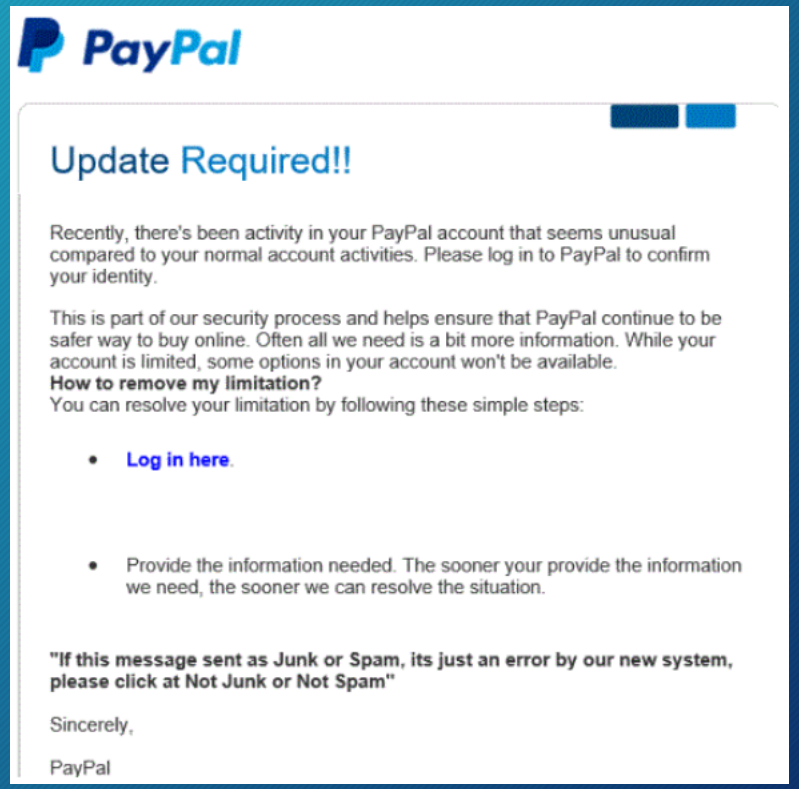
Hameçonnage - Fonctionnement



Hameçonnage - Différentes formes

Vous incitant à :

- Fournir des informations de connexions
- Fournir des données financières
- Cliquer sur un lien pour vous logger



PayPal

Update Required!!

Recently, there's been activity in your PayPal account that seems unusual compared to your normal account activities. Please log in to PayPal to confirm your identity.

This is part of our security process and helps ensure that PayPal continue to be safer way to buy online. Often all we need is a bit more information. While your account is limited, some options in your account won't be available.

How to remove my limitation?

You can resolve your limitation by following these simple steps:

- **Log in here**.
- Provide the information needed. The sooner your provide the information we need, the sooner we can resolve the situation.

"If this message sent as Junk or Spam, its just an error by our new system, please click at Not Junk or Not Spam"

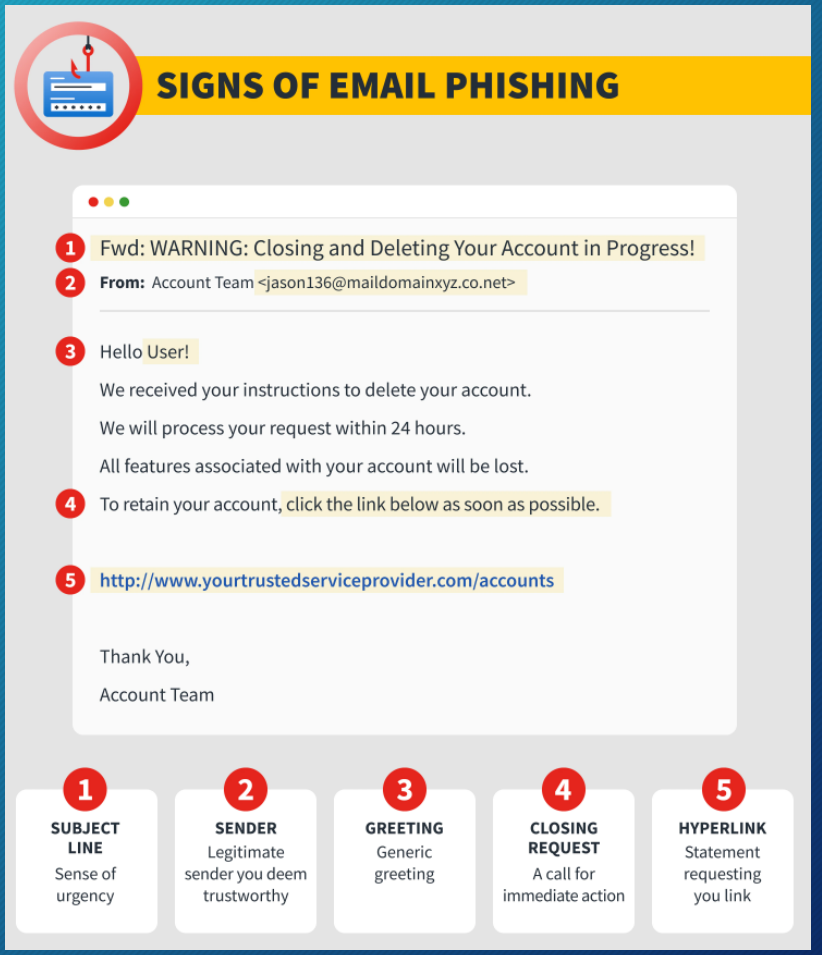
Sincerely,

PayPal

Hameçonnage - Différentes formes

Signes d'email phishing :

- Sujet du mail (Offres, urgent, …)
- Mail émetteur suspect
- Introduction générique
- Requête d'une action (click lien)
- URL du lien / bouton suspect
- Fotes d'ortaugrafe ^_^'



Hameçonnage - Différentes formes

Social engineering → cible spécifique

Améliorer les éléments du mail :
Mail CEO, contexte professionnel, …

Personnes haut placées → Whaling

Version identique d'un e-mail officiel que les victimes ont déjà reçu avec des alternatives frauduleuses

Pub poussant l’achat de logiciel non essentiel en jouant sur la peur de l’utilisateur

Hameçonnage – Se protéger

1. Faire preuve de bon sens
2. N'ouvrez pas les emails suspects
3. Ne cliquez pas sur les liens des mails suspects
4. N'envoyez pas vos informations bancaires par email
5. Ne cliquez pas sur les publicités pop-up
6. Utilisez le filtrage de spam
7. Utilisez une protection anti-virus

https://www.circl.lu/urlabuse/

Sources

https://www.ssi.gouv.fr/uploads/2014/09/anssi_passeport_2019_1.0.pdf
https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf
https://www.ssi.gouv.fr/uploads/2018/10/guide_nomadisme_anssi_pa_054_v1.pdf
https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf
https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
https://finances.belgium.be/fr/phishing
https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html
https://iotindustriel.com/technologies-solutions-iiot/sans-fil/5-dangers-qui-menacent-votre-reseau-sans-fil-industriel/
https://www.kaspersky.fr/resource-center/preemptive-safety/public-wifi-risks
https://cba.ca/wifi-hotspot-scam?l=en-us
http://www.ordinateur.cc/r%C3%A9seaux/r%C3%A9seau-sans-fil/83516.html
https://www.ssi.gouv.fr/uploads/2018/10/guide_nomadisme_anssi_pa_054_v1.pdf

Sortez couverts avec l'ANSSI & la CNIL !!!