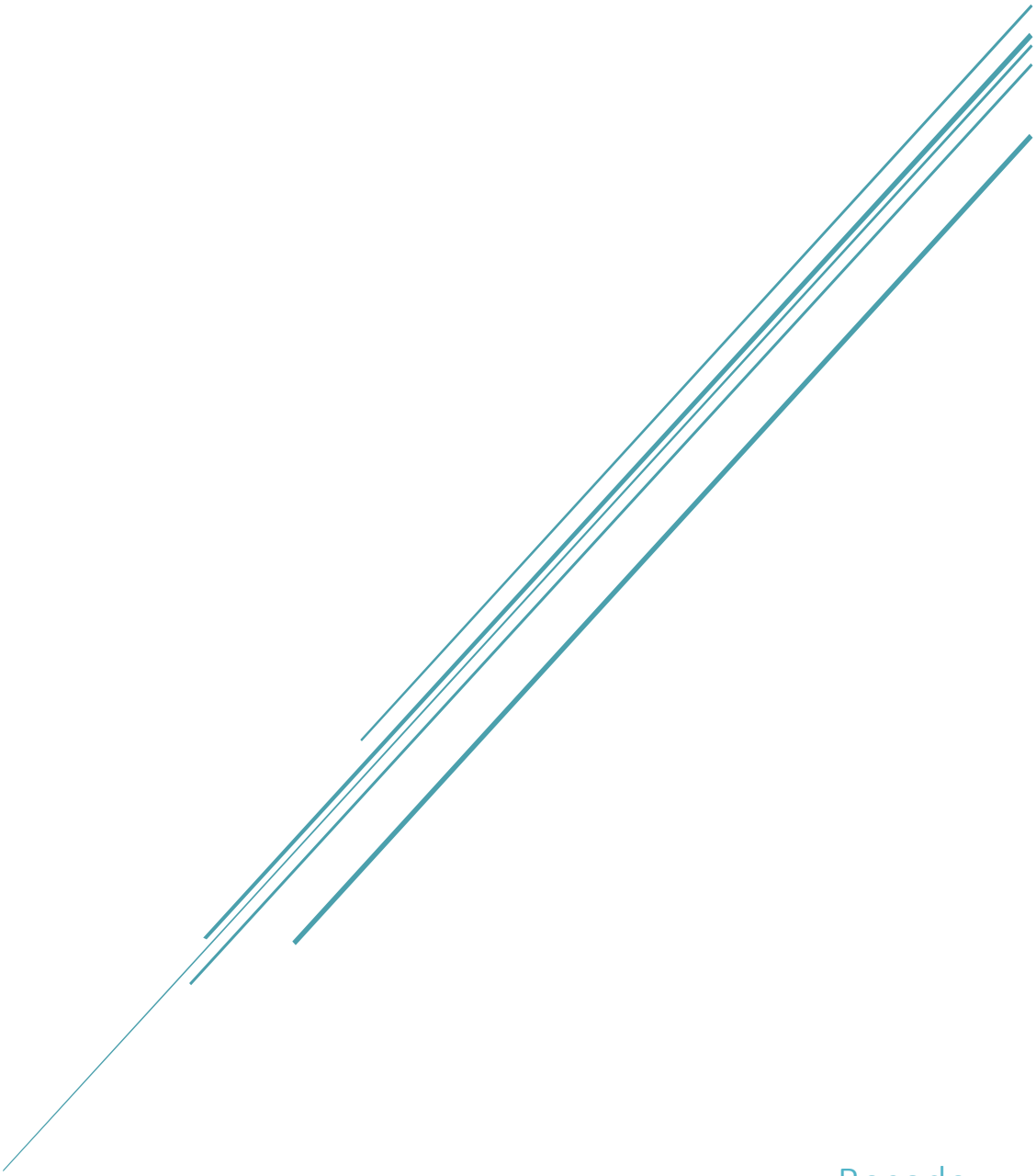
CERTIFICATION TOSA

Wifi, surexposition données, phishing



Becode

Anaïs, Maria, Robin & Greg

TABLE DES MATIERES

1. RÉSEAUX SANS FILS

RISQUES

L'utilisation du Wifi public est dangereuse parce que (*selon les chiffres d'Avira*), 75% d'entre eux sont vulnérables. Ils n'exigent généralement aucune authentification pour établir une connexion, les pirates profitent donc d'un accès gratuit à des appareils non sécurisés connectés au même réseau. Les pirates sont en mesure d'intégrer les réseaux et de piocher dans les données personnelles qui transitent. L'un des risques les plus importants concerne l'interception des informations. Pour cela, le hacker pirate le système et se positionne entre le client et le point d'accès.

Un des risques communs de sécurité du réseau sans fil est causée par l'erreur humaine. Ce risque est créé quand les employés d'une entreprise, par exemple, ne peuvent pas comprendre les risques associés à donner des mots de passe d'accès ou le partage de données. Si les utilisateurs d'un réseau ne suivent pas les politiques intelligentes, les failles de sécurité peuvent se développer.

Les vulnérabilités logicielles permettent également aux attaquants d'injecter à votre insu des malwares sur votre ordinateur. Une vulnérabilité logicielle est une faille de sécurité ou une faiblesse détectée dans un système d'exploitation ou un programme informatique. Les pirates informatiques savent exploiter ces faiblesses en écrivant du code ciblant une vulnérabilité spécifique, code qu'ils injectent ensuite sur votre appareil sous la forme d'un malware.

La connexion Bluetooth permet aux appareils de communiquer entre eux. Les pirates peuvent rechercher des signaux Bluetooth actifs pour accéder à votre appareil.

RECONNAITRE ET UTILISER UN RÉSEAU SANS FIL (WIFI, BLUETOOTH) SÉCURISÉ :

Par exemple, un réseau nommé "Bureau" devrait être remplacé par "23-F3" ou un autre nom obscur. Cela permet d'empêcher les utilisateurs non autorisés de deviner quel réseau est associé à une organisation. Ce nom peut également être modifié périodiquement.

Un réseau sans fil peut être "masqué", l'utilisateur doit entrer le nom exact du réseau au lieu de le sélectionner dans une liste.

Les réseaux sans fil doivent utiliser le chiffrement le plus avancé possible. Car des méthodes de chiffrement obsolètes peuvent être plus facilement contournées par des utilisateurs qualifiés.

Désactiver le partage dans les préférences système ou le panneau de configuration (Windows).

Laisser la fonctionnalité Wifi désactivée lorsqu'on n'en a pas besoin.

Utiliser des connexions SSL qui chiffrent le trafic de bout en bout. Il faut toujours utiliser le protocole HTTPS sur les sites web qui invitent à saisir des données d'identification ou bancaires.

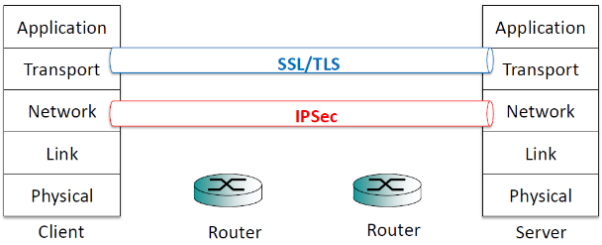
CONNAITRE L'UTILITÉ ET SAVOIR UTILISER UN VPN :

Les VPN permettent de se protéger efficacement sur les Wifi publics. Ils ont la capacité de chiffrer toutes les données qui transitent en créant un tunnel sécurisé entre le client et le serveur VPN.

Il est donc important d'utiliser des mécanismes robustes de chiffrement, d'authentification et d'intégrité pour la mise en place du canal d'interconnexion d'un équipement d'accès nomade. L'ANSSI recommande l'utilisation du protocole IPsec plutôt que TLS pour la mise en place du tunnel VPN entre l'équipement d'accès et l'équipement de terminaison VPN, notamment pour les raisons suivantes :

- La surface d'attaque d'IPsec est plus réduite comparativement à celle de TLS. Les opérations
  de sécurité critiques (comme les fonctions utilisant les clés) d'IPsec se font en environnement
  cloisonné, au sein du noyau du système d'exploitation, tandis que TLS s'exécute généralement
  dans l'espace utilisateur, depuis la couche applicative.
- Les mécanismes de choix initial des algorithmes entre le client et le serveur sont plus robustes en IPsec qu'en TLS. De manière générale, la conception et la séparation des différentes fonctions de sécurité est plus aboutie dans IPsec (définition de SPD [1] et de SA [2] , négociation des échanges de secrets partagés avec le protocole IKE [3], mécanisme de création et modification automatiques de SA avec ISAKMP [4], mécanisme de Re-key et de Re-Auth pour le renouvellement des clés de sessions et la réauthentification).
- La gestion par défaut des autorités de certification autorisées est plus permissive dans les différentes implémentations de TLS que dans celles d'IPsec.
- La majorité des vulnérabilités récentes concerne les implémentations des protocoles SSL et TLS (POODLE, BEAST, CRIME, FREAK, Heartbleed, etc.). De manière générale, ce n'est pas tant le protocole TLS en lui-même qui est source de vulnérabilités, mais plutôt des mauvaises implémentations développées dans des langages qui n'apportent pas toujours un niveau de sécurité satisfaisant.

1 .Security policy database.
2. Security association.
3. Internet key exchange.
4. Internet security association and key management protocol.



Sources :

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

2. SUREXPOSITION DES DONNÉES

Objectif pour la certification : parvenir à distinguer les potentielles sources de fuite de données lors d'un déplacement externe, afin de limiter la diffusion d'informations sensibles.

LES RISQUES LIÉS AUX DÉPLACEMENTS :

Le nomadisme numérique désigne 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 (entreprise, organisation), depuis des lieux distants, ces lieux n'étant pas maîtrisés par l'entité.

Ainsi, la principale caractéristique du nomadisme est le degré d'exposition de l'information, en raison de la localisation de l'utilisateur dans des lieux n'ayant pas les moyens de protection physique habituellement mis en œuvre dans les locaux de l'entité pour laquelle il travaille. C'est le cas par exemple :

- Lorsque l'on travaille à l'hôtel pendant un déplacement professionnel ;
- Pendant le trajet domicile-travail, dans les transports en commun ;
- Lorsque l'on travaille dans des salles d'attentes ou tout autre lieu public ;
- Lorsque l'on se connecte depuis un espace de coworking ;

Dans tous ces lieux de travail non maîtrisés par l'entité, les risques suivants sont exacerbés :

- La perte ou vol de matériel ;
- La compromission du matériel, par exemple pendant une absence temporaire de l'utilisateur ;
- La compromission des informations contenues dans le matériel volé, perdu ou emprunté ;
- 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).

PRÉCONISATIONS AVANT TOUT DÉPLACEMENT :

Le but est d'anticiper l'atteinte à la sécurité des données consécutive au vol ou à la perte d'un équipement mobile lors d'un déplacement ainsi que de limiter l'exposition de données sensibles à l'écrit, à l'oral ou sur écran à l'extérieur. La multiplication des ordinateurs portables, des clés USB et des smartphones rend indispensable d'anticiper les atteintes à la sécurité des données consécutives au vol ou à la perte de tels équipements.

1. EFFECTUER UN TRAVAIL DE SENSIBILISATION :

- Sensibiliser les utilisateurs aux risques spécifiques liés à l'utilisation d'outils informatiques mobiles (ex : vol de matériel) et aux procédures prévues pour les limiter lors de déplacements.

2. EVITER LE TRANSPORT DE DONNÉES SUPERFLUES (S'EN TENIR AUX DONNÉES NÉCESSAIRES) :

- Lors des déplacements, réduire le risque de perte ou de vol de données en emportant le strict minimum sur les équipements nomades (limiter le stockage des données sur les postes nomades au strict nécessaire) et éventuellement interdire le stockage de données lors de déplacement à l'étranger (en fonction de la situation) ;
- Ne pas héberger de données professionnelles sur vos équipements personnels (clé USB, téléphone, etc.) ou sur des moyens personnels de stockage en ligne ;
- De la même façon, il faut éviter de connecter des supports amovibles personnels (clés USB, disques durs externes, etc.) aux ordinateurs de l'entreprise ;
- Se renseigner auprès du responsable de la sécurité l'organisation/entreprise sur les solutions sécurisées disponibles en entreprise (conteneur chiffré, cloud sécurisé, etc.) ;
- Limiter la connexion de supports mobiles (clés USB, disques durs externes, etc.) à l'indispensable ;
- Désactiver l'exécution automatique (« autorun ») depuis des supports amovibles.

3. S'INFORMER SUR LA LÉGISLATION DU PAYS DE DESTINATION :

- Se renseigner auprès du service juridique ou du responsable de la sécurité sur la législation du pays de destination vis-à-vis des moyens de chiffrement ;
- Adapter la sécurisation des moyens de communication et de stockage au cadre réglementaire local et aux besoins de la mission.

4. SAUVEGARDER LES DONNÉES EMPORTÉES :

- La réalisation de sauvegardes garantit la récupération des données en cas d'incident (perte, vol, casse, panne, etc.) sur les équipements (prévoir la mise en œuvre des mécanismes maîtrisés de sauvegardes ou de synchronisation des postes nomades);
- Réaliser des sauvegardes régulières sur un support déconnecté de tout réseau fourni par votre organisation constitue un gage de sécurité supplémentaire.

5. CHIFFRER LES DONNÉES EMPORTÉES :

- Prévoir des moyens de chiffrement des postes nomades et supports de stockage mobiles (ordinateur portable, clés USB, disque dur externes, CD-R, DVD-RW, etc.), par exemple : le chiffrement du disque dur dans sa totalité lorsque le système d'exploitation le propose ; le chiffrement fichier par fichier ; la création de conteneurs (fichier susceptible de contenir plusieurs fichiers) chiffrés.

CE QU'IL NE FAUT PAS FAIRE

- 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.

PRÉCONISATIONS PENDANT TOUT DÉPLACEMENT :

1. FAIRE PREUVE DE DISCRÉTION :

- Éviter autant que possible la consultation de documents sensibles depuis des lieux publics et doter les équipements (ordinateur, tablette, téléphone) d'un filtre de confidentialité ;
- En ligne (photos, commentaires, tweets, etc.) ou dans les lieux publics, toujours évaluer la communication (écrite ou orale) sur les raisons d'un déplacement, mission de travail ou de destination et veiller à la communiquer que lorsque c'est nécessaire ; bien entendu éviter de le faire dans la mesure du possible ;
- Ne donner accès qu'à un minimum (voire pas du tout) d'informations personnelles et professionnelles sur les réseaux sociaux, et être vigilant lors des interactions avec les autres utilisateurs (une attention particulière doit être portée à l'ingénierie sociale, ne pas divulguer d'informations pro ou personnelles à des tiers) ;

2. EVITER DE LAISSER SES DOCUMENTS ET ÉQUIPEMENTS SANS SURVEILLANCE :

- Lors d'un éloignement contraint des équipements, même pendant un temps très court, toujours verrouiller la session de travail (ou configurer au minimum un verrouillage automatique de la session) et mettre en place la purge des données collectées sitôt qu'elles ont été transférées au système d'information de l'organisme ;
- Afin de préserver l'intégrité des équipements en cas d'éloignement, des enveloppes inviolables et câbles antivol pour ordinateurs portables existent et constituent une parade simple dans la plupart des situations usuelles ; En somme, toujours prévoir des mécanismes de protection contre le vol (par ex. câble de sécurité, marquage visible du matériel) et de limitation de ses impacts (par ex. verrouillage automatique, chiffrement) ;
- Concernant les smartphones, en plus du code PIN de la carte SIM, activer le verrouillage automatique du terminal et exiger un secret pour le déverrouiller (mot de passe, schéma, etc.) ;

3. EVITER DE SE CONNECTER AUX RÉSEAUX OU ÉQUIPEMENTS NON MAITRISÉS :

- Pour se connecter à Internet : imposer un VPN pour l'accès à distance ainsi que, si possible, une authentification forte de l'utilisateur (carte à puce, boitier générateur de mots de passe à usage unique (OTP), etc.) ;
- Utiliser les moyens professionnels sécurisés fournis par l'entreprise (téléphone, ordinateur, VPN, etc.). Ne pas les contourner par l'usage de moyens personnels (ex. : messagerie personnelle) ;
- En ce qui concerne les moyens de communication à utiliser en déplacement, utiliser des alias pour les adresses email : essayer d'avoir des adresses de messagerie indépendantes les unes des autres et utiliser des utiliser des systèmes de chiffrement : on va demander des clés PgP à notre destinataire, chiffrer le message avec cette clé et seul le destinataire pourra déchiffrer le contenu de l'email ;
- Utiliser des prestataires fiables (pas comme Google, Outlook qui communiquent les informations privées si on est soucieux de l'anonymat et de la vie privée) par exemple

ProtonMail.com ; Ne pas utiliser, publier ou regrouper des données persos sous une seule adresse e-mail ;

- Ne faites pas suivre vos messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles ;
- Lorsque c'est possible, éviter de se connecter aux réseaux non maîtrisés (Wi-Fi d'hôtel, de gare ou de café, bornes de recharge en libre-service, salle de réunion extérieure, etc.) et garder un antivirus et un pare-feu actif. L'idée est de limiter les flux réseau au strict nécessaire en filtrant les flux entrants/sortants sur les équipements (pare- feu, proxy, serveurs, etc.). Par exemple, si un serveur web utilise obligatoirement HTTPS, il faut autoriser uniquement les flux entrants sur cette machine sur le port 443 et bloquer tous les autres ports) ;
- Si le recours à un service de ce type (Wi-Fi public) est la seule solution disponible, il faut s'abstenir d'y faire transiter toute donnée personnelle ou confidentielle (en particulier messages, transactions financières). Enfin, il n'est pas recommandé de laisser vos clients, fournisseurs ou autres tiers se connecter sur votre réseau (Wi-Fi ou filaire). Ne pas partager sa connexion ;
- Désactiver les fonctions Wi-Fi et Bluetooth des appareils ;
- Retirer la carte SIM et la batterie si vous êtes contraint de vous séparer de votre téléphone ;
- Ne pas utiliser les équipements qui vous sont offerts (clé USB, objet connecté, etc.) sans les avoir fait vérifier par votre responsable sécurité, ils peuvent avoir été piégés.
- Ne jamais utiliser les clés USB qui peuvent avoir été offertes lors de déplacements (salons, réunions, voyages...) : très prisées des attaquants, elles sont susceptibles de contenir des programmes malveillants.

4. INFORMER LE RESPONSABLE DE LA SÉCURITÉ EN CAS DE PERTE OU DE VOL :

- En cas de disparition de l'un des équipements en déplacement ou de son fonctionnement anormal, il faut informer sans délai le responsable de la sécurité de l'entreprise ;
- Il indiquera, selon le contexte, qui contacter sur place voire auprès de qui déposer plainte ;
- Il pourra ainsi prendre sans délai les mesures nécessaires pour protéger de connexions malveillantes le patrimoine informationnel de l'organisation.

PRÉCONISATIONS APRES TOUT DÉPLACEMENT

1. RENOUVELER LES MOTS DE PASSE UTILISÉS LORS DES DÉPLACEMENTS :

- En toutes circonstances et lorsque les équipements et applications le permettent, toujours opter pour une authentification forte (application mobile, clé USB, carte à puce, etc.) ;
- Utiliser un mot de passe différent pour chacun des comptes et équipements (messageries, réseaux sociaux, poste de travail, téléphone mobile, etc.) ;
- Renouveler en priorité les mots de passe utilisés pendant la mission et sur lesquels pèsent un doute.

2. FAIRE VÉRIFIER LES ÉQUIPEMENTS PAR LE RESPONSABLE DE LA SÉCURITÉ :

- Effacez l'historique des appels et de navigation ;
- Après tout retour de mission et de déplacement en général, il est conseillé de confier les équipements au responsable de la sécurité, en particulier en cas de :
    - Saisie de ceux-ci (Police aux frontières, accueil d'une organisation, etc.) durant un déplacement ;
    - En cas de doutes sur l'intégrité de l'un d'eux.

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

3. HAMEÇONNAGE

Le phishing est une technique de cybercriminalité qui utilise la fraude, la supercherie ou la tromperie pour vous inciter à divulguer des informations personnelles sensibles. C'est en fait n'importe quel type de fraude de télécommunications qui utilise des astuces **d'ingénierie sociale** pour obtenir des données confidentielles de la part de leurs victimes.

L'hameçonnage, c'est quand un cybercriminel prétend être une organisation légitime pour essayer d'obtenir des données confidentielles.

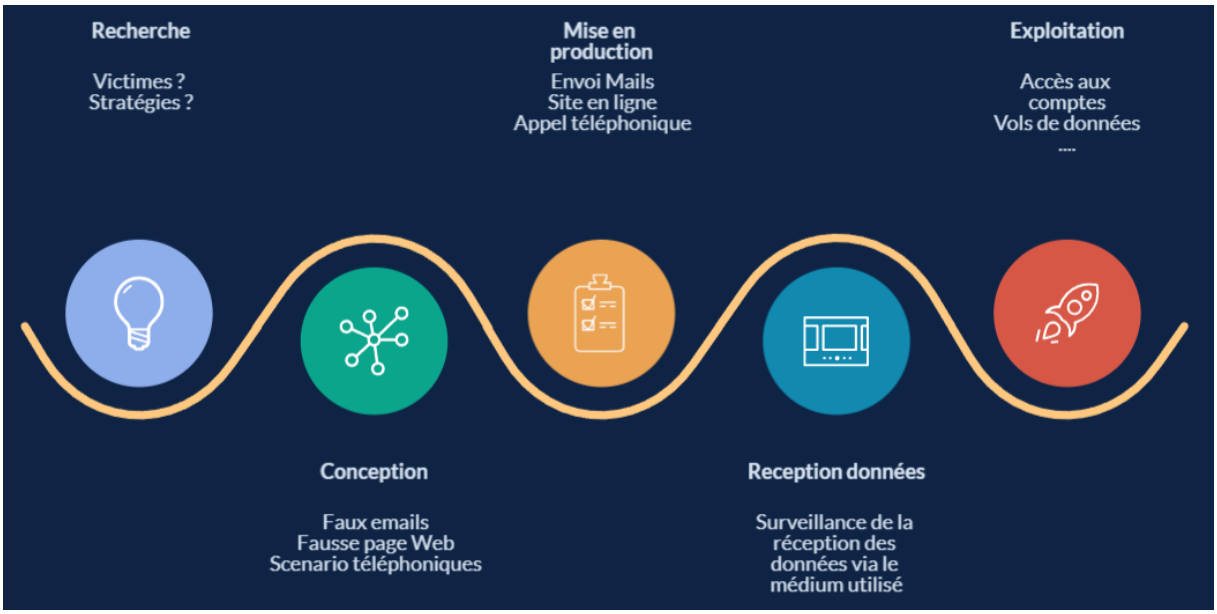
Par exemple, quelqu'un pourrait vous envoyer un courriel ou vous appeler pour vous demander de fournir votre numéro de compte bancaire ou de carte de crédit, ou même vos noms d'utilisateurs ou vos mots de passe.

Cette information peut être utilisée pour accéder à vos comptes importants et peut avoir comme résultat le vol de votre identité ou des pertes financières.

COMMENT LE PHISHING FONCTIONNE-T-IL ?

1. L'arnaqueur détermine tout d'abord qui seront ses victimes (une orga ou un particulier) et met en place une stratégie d'attaque.
2. Ensuite, il va créer de faux emails ou des pages internet douteuses afin d'envoyer des messages qui vont permettre d'intercepter les données de ses victimes.
3. Ces messages, qui vont sembler **dignes de confiance**, vont ensuite être envoyés aux victimes
4. Une fois l'attaque déployée, l'arnaqueur va surveiller la réception des données via le medium employé
5. Pour finir, ces données vont être utilisées par les phishers dans un but frauduleux.

Ceci dit, les attaques d'hameçonnages peuvent prendre différentes formes et être déployées dans différents buts.



LES DIFFÉRENTES FORMES D'HAMEÇONNAGE

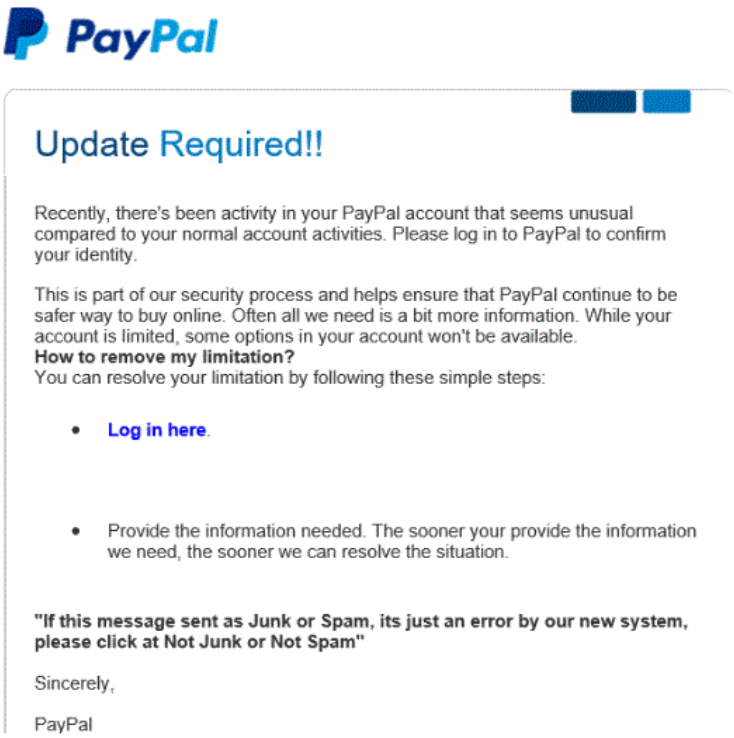
E-MAIL PHISHING

Ces e-mails sont conçus de façon à vous inciter à fournir vos informations de connexion ou vos données financières (n° de carte de crédit, n° de sécurité sociale etc).

D'autres courriels peuvent vous amener à cliquer sur un lien qui mène à un faux site internet au design similaire à celui d'une entreprise connue tel qu'Amazon, eBay ou votre banque. Ces pages web peuvent ensuite installer des programmes malveillants ou des virus directement sur votre machine.

Un exemple : vous pourriez recevoir un e-mail qui semble provenir de PayPal. Le message vous informe que vous devez cliquer sur un lien pour vérifier votre compte PayPal et si vous ne le faites pas, votre compte sera clôturé.

Bien entendu, il s'agit d'une escroquerie. Si vous cliquez sur le lien, vous serez amené à vous logger sur une page qui ressemble au site de paypal. Si vous rentrez vos infos, elles seront récupérées par les escrocs.



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

Ces mails contiennent souvent des fautes d'orthographe, de grammaire et des intro génériques ("Dear User" or "Dear client"). Les liens sur lesquels vous êtes supposés cliquer mèneront souvent à des sites aux URLS étranges, différentes de l'entreprise légitime.

SPEAR PHISHING

Alors que la plupart des mails de phishings sont destinés à un large groupe de personne, il y a un type d'attaque qui est plus personnel par nature, le spear phishing.

Les emails de spear phishing sont destinés à un individu, une entreprise ou une organisation en particulier. A l'inverse des attaques de fraude plus générique, les escrocs qui emploient le spear phishing passent du temps à s'informer sur leurs victimes (social engineering).

Par exemple, un email malveillant peut prendre pour cible les employés d'une boîte. L'expéditeur apparaîtrait comme étant un manager voire le CEO. Le message demanderait accès à des données sensibles de la boîte, conduisant à une fuite des données.

CLONE PHISHING

Le clone phishing est une des techniques des plus difficiles à détecter. Dans ce cas-ci, les escrocs créent une version identique d'un e-mail que les victimes ont déjà reçu.

Le clone est envoyé depuis une adresse mail qui ressemble à celle de l'expéditeur originel mais n'est pas identique. Le corps de texte est quant à lui identique à l'exception de la pièce jointe ou du lien qui ont été remplacés par des alternatives frauduleuses.

WHALING

Comme le spear phishing mais vise des personnes haut placées.

POP-UP PHISHING

Il s'agit de publicités sous forme de fenêtres pop-up qui poussent les internautes à acheter une protection antivirus dont ils n'ont pas besoin. On a recours à la peur dans les messages de ces pop-ups, comme un avertissement signalant que l'ordinateur a été infecté et que la seule façon de se débarrasser du virus est d'installer un type particulier d'antivirus.

COMMENT SE PROTÉGER DES TENTATIVES DE PHISHING?

Règle de base - faire preuve de bon sens

- **N'ouvrez pas les emails suspects.** Si vous recevez un email d'une soi-disant institution financière au titre alarmant - "Compte suspendu !" -, supprimez-le. Si vous vous craignez qu'il y ait un problème, connectez-vous à votre compte via le site de votre banque afin de vérifier.
- **Ne cliquez pas sur les liens des mails suspects.** Si vous ouvrez un email d'un expéditeur inconnu vous invitant à cliquer sur un lien, ne le faites pas. Souvent, ces liens mènent à de faux sites web dont le but est de voler vos données ou installer un malware. Ou bien, vérifiez vos liens : https://www.circl.lu/urlabuse/
- **N'envoyez pas vos informations bancaires par email.** Votre banque ne vous demandera jamais de fournir vos numéros de comptes bancaires ou vos mots de passe par email.
- **Ne cliquez pas sur les publicités pop-up.**
- **Utilisez le filtrage de spam.** La plupart du temps, les boîtes mails utilisent des filtres à spam mais si un courriel passe à travers les mailles du filet et se retrouve dans votre boîte de réception, faites preuve de bon sens.
- **Utilisez une protection anti-virus.** Assurez-vous que votre ordinateur est protégé par un logiciel de sécurité efficace.

Sources :

https://finances.belgium.be/fr/phishing

https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html