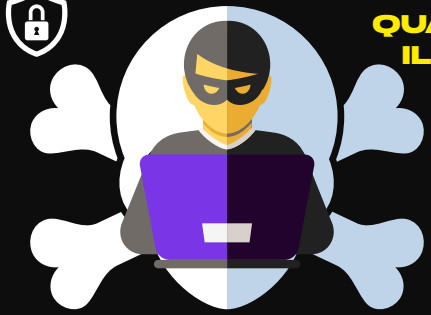
CYBERSÉCURITÉ

Face aux risques liés à la cybercriminalité et quelle que soit votre secteur d'activité, votre sécurité doit être résiliente à toute épreuves.
Ces infractions numériques visant à récupérer vos données de manières frauduleuses sont toutes différentes et peuvent être anticipées.
Vous trouverez ci-dessous les 10 «cyber-malveillances» les plus fréquentes et quelques conseils afin de vous sensibiliser aux mesures prioritaires à mettre en place.



QUAND IL Y A UN DOUTE IL N'Y A PAS DE DOUTE

Faites-vous confiance : si vous avez un doute ou une interrogation, mefiez-vous et suivez nos recommandations.

Ne communiquez jamais d'informations sensibles par messagerie ou téléphone.

HAMEÇONNAGE

Principale cybermalveillance rencontrée, tous publics confondus, l'hameçonnage ou le phishing cible la victime par l'envoi d'un mail ou sms l'incitant à réaliser une action tel que : l'ouverture d'un lien ou d'une pièce jointe infectée par un virus. Cette cyber attaque consiste à leurrer l'internaute en l'incitant à communiquer des données personnelles (comptes d'accès, mots de passe...) et/ou bancaires en se faisant passer pour un tiers de confiance.

PIRATAGE DE COMPTE

Seconde menace la plus rencontrée, le piratage de compte en ligne s'oriente aujourd'hui principalement vers l'attaque de compte de messagerie.
En effet, les cybercriminels l'ont compris, les messageries sont généralement les points centraux par lesquels transitent toutes les informations de réinitialisation de mots de passe ou de comptes en ligne.

ARNAQUE AUX FAUX SUPPORTS TECHNIQUE

Ce piège vise principalement les séniors, plus novices en matière de pratiques numériques. Il consiste à bloquer l'ordinateur de la victime en y faisant apparaitre un message évoquant une faille ou un incident et l'invitant à se rapprocher d'un support technique malveillant. Son but ? Récupérer les codes d'accès via la prise en main de l'appareil et d'en faire par la suite un usage frauduleux.

CYBERHARCÈLEMENT

Il peut se manifester sous différentes formes : intimidations, insultes, menaces, rumeurs, publications de photos...
Ces comportements ont pour but la dégradation des conditions de vie de la victime et s'accompagnent régulièrement de chantages financiers.

VIOLATION DE DONNÉES PERSONNELLES

Vos données personnelles sont des informations clés permettant l'identification directe d'une personnes : photos, nom, adresse, mail, adresse IP...
Ainsi, la violation ou l'usurpation des données personnelles peut avoir des conséquences lourdes, préjudices financier, atteinte à la réputation, tentative d'hameçonnage...

SÉCURISER

- Utiliser un antivirus
- Protégez vos accès par des mots de passes solides.
- Sauvegardez vos données régulièrement
- Appliquez vos mises à jour de sécurité

VÉRIFIER

- Méfiez-vous des mails inattendus
- Vérifier les liens ou pièces jointes si vous avez un doute : https://www.virusto-tal.com
- Contrôlez l'url des sites sur lesquels vous faites vos achats
- Téléchargez vos applications sur des

SE FAIRE ACCOMPAGNER

- Si le doute persiste ou si vous êtes victime d'une cyberattaque :
- Ne communiquez aucune information !
- Changez vos mots de passe
- Faites opposition
- Faites-vous assister par un professionnel

CONTACTEZ-NOUS

RANÇONGICIEL

L'attaque du cybercriminel vise à bloquer l'accès à l'appareil de l'utilisateur ou à certains fichiers en l'échange d'une rançon pour en obtenir de nouveau l'accès. Ces rançongiciels constituent la principale attaque chez les professionnels.

SPAM

Non sollicité et à des fins commerciales ou malveillantes, le spam peut prendre plusieures formes : sms, email, réseaux sociaux...Généralement agissant comme outil de prospection commerciale, faites preuve de vigilance car il peut être malveillant : demande de rappel à un numéro surtaxé, tentative de phishing, escroquerie et/ou piratage...

ATTAQUES EN DÉNI DE SERVICE

Cela vise à saturer un serveur afin de le rendre inaccessible ou bien à exploiter une faille de sécurité qui permettrait de dégrader voir d'interrompre le service/site. Le but d'une telle manoeuvre étant de descréditer et de nuir à la réputation de la victime.

FAUX ORDRES DE VIREMENT

Cyberattaque consistant à tromper la victime pour la pousser à réaliser un virement de fonds sur un compte détenu par un cybercriminel. «L'arnaque au président» est l'un des modes opératoire les plus courants : il s'agit d'une demande de virement urgente et confidentielle émanant d'un dirigeant. Dans la majeure partie des cas, cette fraude fait suite à un piratage et/ou à une usurpation d'identité.

VIRUS

On ne le présente plus, le virus est un programme informatique malveillant dont l'objectif est de s'implenter sur un système informatique afin d'en perturber son fonctionnement et de nuire à la cybersécurité de son propriétaire.
Il s'infiltre par l'ouverture d'un mail, d'une pièce jointe ou d'un clic sur un lien et se manifeste par un ralentissement, un blocage.

ABBANA