Revisium

MENACES Cybersécurité

Tendances et risques

2024

0 805 035 135
www.revisium.fr

Hameçonnage

Définition

L’hameçonnage (phishing en anglais) est une technique frauduleuse destinée à leurrer l’internaute pour l’inciter à communiquer des données personnelles (comptes d’accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance. Il peut s’agir d’un faux message, SMS ou appel téléphonique de banque, de réseau social, d’opérateur de téléphonie, de fournisseur d’énergie, de site de commerce en ligne, d’administrations, etc.

Se prémunir

- **Ne communiquez jamais d’informations sensibles par messagerie ou téléphone**
- **Avant de cliquer sur un lien douteux, positionnez le curseur de votre soucis sur ce lien sans cliquer pour afficher l’adresse réelle du site**
- **Vérifier systématiquement l’adresse du site qui s’affiche dans votre navigateur si vous avez cliqué**
- **En cas de doute, contactez si possible directement l’interlocuteur ou l’organisme concerné**
- **Utilisez des mots de passe différents et complexes pour chaque site et application que vous utilisez (idéalement optez pour un gestionnaire de mots de passe)**
- **Vérifier la date et l’heure de dernière connexion à votre compte pour repérer des accès illégitimes**
- **Si possible, activez la double authentification**

Bon à savoir

Pour être conseillé en cas d’hameçonnage, contactez INFO ESCROQUERIES au 0 805 805 817 (numéro gratuit).

Rançongiciel

Définition

Un rançongiciel (ransomware en anglais) est un logiciel malveillant qui bloque l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès. La machine peut être infectée après l'ouverture d'une pièce jointe, ou après avoir cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en naviguant sur des sites compromis, ou encore suite à une intrusion sur le système. Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes.

Se prémunir

- **Appliquez de manière régulière et systématique les mises à jour de sécurité**
- **Tenez à jour l'antivirus et configurez votre pare-feu**
- **N'ouvrez jamais les courriels, leurs pièces jointes et ne cliquez pas sur les liens provenant des chaînes de messages ou d'expéditeurs inconnus**
- **N'installez pas d'application ou de programme non vérifiés**
- **Evitez les sites illicites ou non sûrs**
- **Faites des sauvegardes régulières de vos données et du système**
- **N'utilisez pas un compte avec des droits administrateur pour consulter des sites ou naviguer sur le web**
- **Utilisez des mots de passe suffisamment complexes et changez-les régulièrement**
- **Eteignez votre machine quand vous ne vous en servez pas**

Conseil

Conservez les preuves pour l'enquête post-piratage et déposez plainte à la gendarmerie ou la police.

Faux support

Définition

L’arnaque au faux support technique (Tech support scam en anglais) consiste à effrayer la victime, par SMS, téléphone, chat, courriel, ou par l’apparition d’un message qui bloque son ordinateur, lui indiquant un problème technique grave et un risque de perte de ses données ou de l’usage de son équipement afin de la pousser à contacter un prétendu support technique officiel, pour ensuite la convaincre de payer un pseudo-dépannage informatique et/ou à acheter des logiciels inutiles, voire nuisibles. Si la victime refuse de payer, les criminels peuvent la menacer de détruire ses fichiers ou de divulguer ses informations personnelles.

Se prémunir

- **Appliquez de manière régulière et systématique les mises à jour de sécurité**
- **Tenez à jour l’antivirus et configurez votre pare-feu**
- **N’installez pas d’application ou de programme non vérifiés**
- **Evitez les sites illicites ou non sûrs**
- **Faites des sauvegardes régulières de vos données et du système**
- **N’utilisez pas un compte avec des droits administrateur pour consulter des sites ou naviguer sur le web**
- **N’ouvrez pas les courriels, les pièces jointes et ne cliquez pas sur les liens**
- **Un support technique officiel ne vous contactera jamais pour vous réclamer de l’argent**

Conseil

Déposez plainte à la gendarmerie ou la police et conservez toutes les preuves de l’arnaque pour l’enquête

Malware

Définition

Un logiciel malveillant ou maliciel, aussi dénommé logiciel nuisible ou programme malveillant ou pourriciel, est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté.

Un malware peut être un cheval de Troie, un ver, un virus, ou encore un maldocs (documents malveillants)

Se prémunir

- **Vérifiez l’authenticité du site internet sur lequel vous êtes envoyé pour télécharger un document ou ouvrir une pièce jointe**
- **Effectuez les mises à jour de sécurité dès qu’elles sont mises en ligne**
- **Montrez une grande méfiance envers mes pièces jointes non sollicitées ou provenant d’adresse d’expéditeurs non identifiés**
- **Bloquez les publicités**
- **Préférez les sources officielles pour le téléchargement de logiciels ou d’outils professionnels**
- **Installez un logiciel anti-malware, un anti-virus et un pare-feu fonctionnels**
- **N’oubliez pas de sécuriser vos appareils connectés !**

Conseil

On oublie souvent que les objets connectés sont une bonne porte ouverte pour les cybercriminels...

Piratage

Définition

Le piratage de compte désigne la prise de contrôle par un individu malveillant d'un compte au détriment de son propriétaire légitime. Il peut s'agir de comptes ou d'applications de messagerie, d'un réseau social, de sites administratifs, de plateformes de commerce en ligne.

Se prémunir

- **Utilisez des mots de passe fort et complexes**
- **Activez la double authentification si possible**
- **Ne communiquez jamais des informations sensibles par messagerie, par téléphone ou sur internet**
- **Appliquez de manière régulière et systématique les mises à jour de sécurité**
- **Maintenez à jour votre antivirus et votre pare-feu**
- **N'ouvrez pas les courriels et les pièces jointes suspectes**
- **Evitez de vous connecter sur un wifi public ou non sécurisé**
- **Déconnectez-vous systématiquement de votre compte après utilisation**

Conseil

Contactez rapidement le site ou le réseau piraté et entamez la procédure de réinitialisation de mot de passe.

Cyberharcèlement

Définition

Le cyberharcèlement consiste en des agissements malveillants répétés, dans un cadre public ou restreint, qui peuvent prendre différentes formes : intimidations, insultes, menaces, rumeurs, publication de photos ou vidéos compromettantes, etc. Ils peuvent être le fait d'une seule personne ou de plusieurs individus et se dérouler sur les réseaux sociaux, messageries, forums, blogs, etc. Les conséquences du cyberharcèlement peuvent être dramatiques pour les victimes.

Se prémunir

- **Vérifiez régulièrement vos paramètres de confidentialité de tous vos comptes**
- **Ne renseignez votre profil qu'avec le minimum d'informations nécessaires**
- **Dans la mesure du possible, maîtrisez vos cercles de connaissances**
- **Maîtrisez vos publications sur les réseaux et sur le web**
- **Soyez très vigilant quand vous communiquez des informations personnelles, intimes et/ou sensibles**
- **Faites preuve de discernement avec certaines inforamtiosn relayées et vérifiez-les avant**

Conseil

En cas de cyberharcèlement, parlez-en, signalez les contenus, conservez les preuves, déposez plainte, et protégez-vous.

Faux conseiller

Définition

La fraude au faux conseiller bancaire désigne un type d'escroquerie qui consiste à tromper la victime pour lui faire valider des opérations frauduleuses sur ses comptes. Il appelle sur votre smartphone pour vous demander vos identifiants ou bien pour vous demander de vous connecter en même temps afin qu'il puisse faire une copie de votre écran et récupérer vos données.

Se prémunir

- **Vérifier les comptes bancaires régulièrement pour détecter rapidement les anomalies**
- **Modifier régulièrement votre mot de passe**
- **Faire les mises à jour de sécurité sur le smartphone et l'ordinateur**
- **Posez des questions si vous avez la personne au téléphone. Si elle devient agressive ou si vous avez la moindre doute, raccrochez !**
- **Votre conseiller ne vous demandera jamais de vous connecter en ligne car il a accès depuis son ordinateur à vos données bancaires**
- **Soyez vigilant également à l'heure d'appel**

Conseil

Signalez tous les faits frauduleux sur le site Perceval du gouvernement. Cela permet d'obtenir une preuve pour la banque.

Défiguration

Définition

La défiguration de site web est l’altération par un pirate de l’apparence d’un site Internet, qui peut devenir uniformément noir, blanc ou comporter des messages, des images, des logos ou des vidéos sans rapport avec l’objet initial du site, voire une courte mention comme « owned » ou « hacked ». La défiguration est le signe visible qu’un site Internet a été attaqué et que l’attaquant en a obtenu les droits lui permettant d’en modifier le contenu. Durant l’attaque, le site n’est souvent plus utilisable, ce qui peut entraîner des pertes directes de revenus et de productivité.

Se prémunir

- **Appliquez de manière régulière et systématique les mises à jour de sécurité du système d’exploitation et des logiciels sur les serveurs**
- **Installez un pare-feu et paramétrez-le**
- **Consultez régulièreent les fichiers de journalisation (logs)**
- **Vérifiez les mots de passe et changez-les pour les mots complexes et robustes**
- **Sensibilisez les utilisateurs à ne jamais communiquer certains éléments d’accès administrateurs et d’authentification à un tiers non identifié**
- **Ne conservez pas de manière accessible la liste nominative des personnes possédant des droits administrateurs**

Conseil

N’éteignez pas l’ordinateur, vous risquez de perdre des données. Coupez l’accès à internet rapidement .

Fraude à la CB

Définition

La fraude à la carte bancaire désigne l'utilisation frauduleuse des coordonnées de la carte bancaire d'une personne à son insu alors que celle-ci est pourtant toujours en possession de sa carte. Trouver l'origine précise d'une telle fraude est souvent difficile. En effet, pour obtenir les coordonnées de la carte bancaire de la victime, le fraudeur peut utiliser de nombreuses méthodes : l'hameçonnage (phishing en anglais) à travers un message incitant la victime à fournir ses coordonnées, le piratage d'un compte en ligne ou d'un équipement, etc.

Se prémunir

- **Ne communiquez jamais vos coordonnées bancaires par téléphone à un tiers**
- **Vérifiez régulièrement votre compte bancaire et les mouvements our identifier les débits suspects**
- **N'enregistrez pas vos coordonnées bancaires dans les sites de vente en ligne**
- **Privilégiez les moyens de paiement sécurisés comme les e-cartes ou encore Paylib**
- **Soyez très vigilant aux demandes de validation si vous n'avez pas réalisé d'achats en ligne**
- **Evitez de vous connecter à un ordianteur depuis un réseau non sécurisé ou un Wifi public**

Conseil

Si vous êtes victime, faites immédiatement opposition à votre carte bancaire et signalez la fraude sur Perceval.

Fraude au président

Définition

La fraude au président est une escroquerie numérique qui se s'étend de plus en plus dans les entreprises. Elle est couplée à la fraude au virement bancaire et inflige à l'entreprise de lourds préjudices pour s'élever à plusieurs millions d'euros.

Ce type d'escroquerie est l'œuvre d'organisations criminelles qui préparent minutieusement leur approche des entreprises. Les fraudeurs connaissent bien la société cible, son activité, ses projets, grâce aux informations ouvertes disponibles sur internet.

Se prémunir

- **Rappelez à l'ensemble des collaborateurs la nécessité d'avoir un usage prudent des réseaux sociaux privés et professionnels**
- **Alertez sur l'importance de ne pas divulguer d'informations concernant le fonctionnement de l'entreprise**
- **Sensibilisez régulièrement le personnel à ce type d'escroquerie. Prenez l'habitude d'en informer systématiquement les nouveaux arrivants et les stagiaires**
- **Instaurez des procédures de vérifications et de signatures multiples pour les paiements internationaux**
- **Maintenez à jour le système de sécurité informatique**
- **Accentuez la vigilance sur les périodes de congés scolaires, les jours fériés, les vendredis soir et les week-ends**

Conseil

En aucun cas vous ne devez accélérer la procédure à cause d'une personne qui vous met la pression... ce n'est pas normal !

Faux virement

Définition

L’escroquerie au virement ou arnaque au faux RIB a pour objectif de tromper la victime, en usurpant l’identité d’un créancier avec lequel elle est en relation (artisan, notaire, avocat, propriétaire/bailleur…), afin de lui faire réaliser un virement vers un compte bancaire détenu par un escroc.
Ce type d’escroquerie est souvent consécutif au piratage d’un compte de messagerie (mail).

Se prémunir

- **Contactez directement votre créancier pour toute demande de virement sur un nouveau RIB reçu par message**
- **Méfiez-vous des messages qui vous incitent à communiquer votre mot de passe de messagerie**
- **Changez régulièrement vos mots de passe et utilisez des mots de passe complexes**
- **Appliquez régulièrement les mises à jour**
- **N’installez pas d’applications ou de logiciels provenant de sources non officielles**
- **Utilisez ouo mettez en place des procédures strictes de réalisation de virements**

Conseil

Si vous êtes victime, alertez immédiatement votre banque de l’opération frauduleuse pour demander une suspension.

Smishing

Définition

Smishing est la contraction de SMS et Phishing. Il s'agit d'une forme de hameçonnage qui utilise le SMS. Les hackers fondent leurs attaques sur l'ingénierie sociale. Elles consistent à induire en erreur les utilisateurs en leur faisant croire que le message reçu est vrai. L'hameçonnage par SMS fonctionne de la même façon qu'un mail frauduleux. Le hacker vous envoie un SMS qui usurpe l'image ou l'identité d'une organisation ou d'une entreprise.

Se prémunir

- **Renseignez-vous sur les solutions de cybersécurité spécifiques aux mobiles - sachez que les systèmes en place disposent déjà de certaines protections natives**
- **Soyez attentif à la pression d'urgence que vous donne le SMS**
- **Effectuez les mises à jour dès qu'elles se présentent**
- **Respectez les bonnes pratiques quant à l'utilisation des smartphones en entreprise**
- **Vérifiez, quand c'est possible, sur internet plutôt que de répondre directement au SMS**

Conseil

Pensez à signaler les SMS frauduleux en vous rendant sur le site 33700.fr du gouvernement.

Ver ou virus

Définition

Un virus est un programme informatique malveillant dont l'objectif est de perturber le fonctionnement normal d'un système informatique à l'insu de son propriétaire. Il existe différents types de virus comme le rançongiciel, le cheval de Troie, le logiciel espion... Les virus peuvent s'infiltrer dans un système informatique par l'ouverture d'un message (mail, MMS, chat), d'une pièce jointe ou d'un clic sur un lien frauduleux, par exemple.

Se prémunir

- **Utilisez un anti-virus et mettez-le à jour régulièrement**
- **N'installez pas de logiciels, programmes ou applications provenant de sources non vérifiées ou non officielles**
- **N'ouvrez pas les messages suspects ni les pièces jointes, et ne cliquez pas sur les liens**
- **Evitez les sites non sûrs ou illicites**
- **N'utilisez pas un compte avec des droits administrateurs pour naviguer sur le web ou pour consulter vos messages**
- **Faites des sauvegardes régulières de vos systèmes et vos données**
- **N'utilisez pas de supports amovibles (clés usb, disque dur externe, autre, etc.) si vous ne connaissez pas la provenance**

Conseil

Si vous suspectez un virus, formatez votre outil et procédez à une restauration du système. Pensez aux sauvegardes !

Ingénierie sociale

Définition

Il existe une autre façon de s'introduire dans les organisations et les réseaux : profiter des faiblesses humaines. C'est ce qu'on appelle l'ingénierie sociale, une technique qui permet d'accéder à des informations ou à des réseaux de données grâce à une technique de manipulation. Par exemple, un intrus peut se présenter comme le personnel du service d'assistance informatique et demander aux utilisateurs de fournir des données, comme leurs noms d'utilisateur et leurs mots de passe. On trouve la technique de l'appât, le prétexte ou encore l'hameçonnage, le spam ou le piratage de la messagerie...

Se prémunir

- **Vérifiez toujours les sources des informations que vous voulez utiliser ou que vous recevez**
- **Ne croyez pas sur parole les informations qu'on vous donne, demandez des preuves, des noms, des détails**
- **Si vous vous sentez piégé ou mal à l'aise, écoutez vos sentiments, ils sont un bon guide**
- **L'urgence n'est pas non plus un bon sentiment et le signe qu'il faut être prudent**
- **Si c'est trop beau pour être vrai, alors ce n'est pas vrai !**

Conseil

Les sentiments sont un élément puissant qui est souvent utilisé, n'y succombez pas !

Vol de données

Définition

Une fuite ou violation de données personnelles est l'accès ou la divulgation non autorisés d'informations personnelles détenues par un tiers (sites Internet, services en ligne, entreprises, associations, collectivités, administrations). L'origine de la fuite peut être accidentelle ou malveillante, interne ou externe à l'organisation qui détient ces données.

Une donnée personnelle désigne une information susceptible d'identifier directement ou indirectement une personne (nom, adresse postale, adresse de messagerie, numéro de téléphone, numéro de sécurité sociale...).

Se prémunir

- **Dans la mesure du possible, ne communiquez qu'un minimum d'informations personnelles**
- **Ne communiquez pas de documents d'identité à n'importe qui**
- **N'enregistrez pas vos coordonnées bancaires dans les sites ecommerce, et préférez retaper les données sans sauvegarde**
- **Utilisez des mots de passe complexes**
- **Activez la double authentification pour augmenter le niveau de sécurité**
- **Désabonnez-vous ou supprimer vos données des comptes que vous n'utilisez plus**

Conseil

Les entreprises sont soumises aux lois européennes du RGPD, pour la gestion des données. Utilisez vos droits !

Usurpation

Définition

L’usurpation d’identité est un délit qui désigne l’utilisation d’informations personnelles permettant d’identifier une personne sans son accord pour réaliser des actions frauduleuses.
En pratique, ces informations ont pu être obtenues par les cybercriminels suite à la perte ou au vol de documents d’identité de la victime, par le biais d’un message d’hameçonnage (phishing en anglais), par le piratage d’un de ses comptes en ligne ou d’un de ses appareils ou encore le piratage d’un site Internet sur lequel ces informations étaient enregistrées, ou même récupérés dans les poubelles de la victime.

Se prémunir

- **Limitez la diffusion de vos données personnelles et sensibles au minimum**
- **Appliquez un filigrane sur vos données d’identité quand c’est possible**
- **Faites attention à qui vous parlez sur internet et par téléphone**
- **Vérifiez vos paramètres de confidentialité de vos informations personnelles sur le web, les réseaux et les applications utilisées**
- **Conservez vos informations personnelles et bancaires en lieu sûr**
- **Détruisez les documents qui contiennent des informations personnelles avant de les jeter (y compris en version papier)**
- **Activez la double authentification sur les sites quand c’est possible**
- **N’ouvrez pas les messages qui vous paraissent suspects et ne cliquez pas sur les pièces jointes**

Bon à savoir

L’usurpation d’identité est une infraction punie par la loi d’un an de prison et 15 000 euros d’amende.

Espionnage

Définition

Les logiciels de surveillance permettent de surveiller à distance les activités, les communications et les déplacements d'une personne sans son accord/sans qu'elle ne s'en rende compte. Ces logiciels peuvent donner accès à différentes fonctionnalités : appels, messages, photos, vidéos, localisation, utilisation des applications, etc.

Se prémunir

- **Changez le code PIN de votre smartphone (ou de votre carte SIM) si vous avez le moindre doute**
- **Utilisez un code de déverrouillage afin que votre smartphone se verrouille après une période d'inactivité**
- **Renforcez vos mots de passe et changez-les au moindre doute**
- **Désactivez le bluetooth, le GPS ou encore le Wifi si vous sortez**
- **Vérifiez les applications installées sur votre smartphone (et pas seulement celles qui sont visibles sur votre écran)**
- **Installez un cache-cam sur votre ordinateur, votre portable ou votre smartphone**
- **Au moindre doute, demandez une analyse de votre smartphone (ou lancez un scan sur votre ordinateur) auprès d'un tiers de confiance**

Conseil

Si vous devez laisser votre ordinateur sans surveillance, verrouillez-le. Il faut un accès physique pour installer un programme...

Spam

Définition

Le spam électronique, également appelé courrier indésirable ou pourriel, désigne une communication électronique non sollicitée à des fins publicitaires, commerciales ou malveillantes. Dans la majorité des cas, il s'agit de messages de prospection commerciale ne respectant pas les obligations légales en matière de consentement des destinataires, mais il peut également revêtir un caractère malveillant : astuces pour gagner de l'argent, sollicitation pour transférer des fonds ou encore tentatives d'hameçonnage (phishing en anglais).

Se prémunir

- **Soyez très vigilant lorsque vous communiquez votre adresse de messagerie à des tiers**
- **Ne répondez pas aux messages dont vous ne connaissez pas l'expéditeur**
- **N'ouvrez pas les courriels ou les pièces jointes provenant des chaînes de messages**
- **Utilisez un filtre ou un logiciel anti-spam**
- **Soyez vigilant quand vous remplissez des formulaires d'inscription ou des bons de commande…**
- **D'abonnez-vous ou supprimer les comptes que nous n'utilisez plus**

Conseil

Signalez tout message suspect sur la plateforme Signal Spam et ne cliquez sur aucun lien.

Bot malveillant

Définition

S’il existe des « bons » bots qui offrent des services utiles (par exemple, Googlebot et Bingbot, qui aident à indexer votre site par les deux principaux moteurs de recherche pour que les clients potentiels puissent vous trouver), les bots malveillants peuvent causer toutes sortes de dommages à votre site et à votre entreprise, en tentant une attaque DDoS, en recherchant des inforamtions privées sur votre site, en republiant votre contenu ailleurs, en transformant vos appareils infectés en appareils zombies.

Se prémunir

- **Investissez dans une solution de gestion de bots, car tous les bots ne sont pas malveillants et certains sont même utiles**
- **Réduisez la bande passage qui lui est allouée pour rendre son fonctionnement nettement moins efficace**
- **Installez un CAPTCHA sur le site (ou des tests invisibles) pour l’empêcher d’agir**
- **Selon votre stratégie, la meilleure approche consiste à bloquer complètement l’activité du bot**

Conseil

Les bots sont de plus en plus sophistiqués alors armez-vous d’outils numériques récents et mis à jour.

Attaque DDoS

Définition

Une attaque en déni de service ou en déni de service distribué (DDoS pour Distributed Denial of Service en anglais) vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service. Ce type d'attaque peut être d'une grande gravité pour l'organisation qui en est victime. Durant l'attaque, le site ou service n'est plus utilisable, au moins temporairement, ou difficilement, ce qui peut entraîner des pertes directes de revenus pour les sites marchands et des pertes de productivité.

Se prémunir

- **Appliquez de manière régulière et systématique les mises à jour de sécurité**
- **Installez un pare-feu et paramétrez-le**
- **Vérifiez que vos mots de passe sont suffisamment forts**
- **Changez régulièrement vos mots de passe**
- **Sollicitez votre hébergeur afin qu'il prévoie une réponse à ce type d'attaque au niveau de ses infrastructures**

Conseil

Ne payez pas de rançon s'il vous en est demandé une. Conservez les preuves et déposez plainte rapidement.

Revisium

CONTACT

Cybersécurité

DPO externe

contact@revisium.fr

Audrey SCHOETTEL
DPO externe & cybersécurité

0 805 035 135
www.revisium.fr