English below

Bonnes pratiques
Anti-Fraude et Sécurité de l'Information

> ANTI-FRAUDE

Tous les jours, vous procédez à des opérations bancaires au travers de plusieurs moyens technologiques ou non comme internet, le téléphone, dans les agences bancaires ou par les différents moyens de paiements en ligne.

Cependant, vous augmentez inévitablement les risques de subir des fraudes bancaires par l'utilisation de tous ces services à votre disposition. Ainsi, ces opérations nécessitent de prendre un certain nombre de mesures simples et efficaces afin de les réaliser dans de bonnes conditions de sécurité.

Société Générale Factoring veille à vous munir un niveau de sécurité élevé pour que vous puissiez naviguer sur vos comptes et réaliser les actions bancaires en toute sérénité.

En tant que client, vous êtes le premier acteur dans la protection de vos données personnelles et bancaires. Par conséquent, il est important de bien connaître les différents risques de fraude au travers de différents exemples d'attaques informatiques dans le chapitre suivant (Sécurité de l'Information) afin de s'en prémunir.

Sachez qu'aucun organisme bancaire ou autres organismes privés ou publics, ne vous demanderont par téléphone ou par mail vos données personnelles, comme les codes de carte bleue, les mots de passe, identifiants etc., car ce sont des données confidentielles et dont vous êtes le seul propriétaire.

En cas de doute, veuillez contacter SG Factoring via le numéro officiel (et non sur le mail que vous avez reçu au cas où) afin de vérifier la véracité de cette demande, en vue de vous prémunir d'une potentielle fraude à votre encontre.

Si vous pensez avoir été victime de fraude, contactez SG Factoring rapidement et déposez plainte auprès des forces de l'ordre.

Les informations bancaires :

L'ensemble de vos codes à usage unique, mots de passe et identifiants servant soit à vous connecter sur votre espace client, soit à réaliser des transactions sur le site internet ou application de votre banque sont des données confidentielles et sensibles. Ainsi, ils ne doivent jamais être communiqués à quiconque afin d'éviter les fraudes bancaires.

Toutes les informations liées à votre compte bancaire, carte bancaire sont également sensibles et confidentielles et doivent être protégées face aux tentatives de fraude.

Les données personnelles :

Vos données personnelles sont aussi des éléments à protéger face au risque de fraude car couplé avec les données bancaires, les individus malveillants les utiliseront afin de commettre différents types d'attaques informatiques. Ces données personnelles, par exemple, sont :

- Nom et prénom
- Adresse postale
- Date de naissance
- Numéro de téléphone
- Adresse mail

Comment les protéger ?

- Evitez de noter sur papier vos codes d'accès, numéros de carte bleue ou mots de passe associés
- Refusez la mémorisation des mots de passe quel que soit l'ordinateur que vous utilisez
- Ne communiquez jamais à un tiers non identifié ou dont la réputation n'est pas sûre des informations bancaires ou personnelles telles que numéros de comptes bancaires, email ou téléphone
- Ne communiquez vos données bancaires que sur des sites fiables et à travers des modes de communications sécurisés (https)
- Evitez de transmettre vos données bancaires par email et messagerie instantanée
- Signalez sans délai à votre banque toute modification illégitime de vos informations personnelles
- Supprimez régulièrement les cookies et fichiers Internet temporaires de votre ordinateur.

> SECURITE DE L'INFORMATION

> Les malwares

Terme :

Malware vient du mot en anglais « malicious software » qui se traduit par « logiciel malveillant ». Vous entendrez souvent le mot « virus » pour désigner les logiciels malveillants mais c'est un terme qui est utilisé abusivement. Cela vient du fait que les premiers logiciels malveillants étaient des virus.

Objectif :

1. Vendre un produit, en passant par l'enregistrement de votre navigation sur Internet pour mieux cibler vos habitudes.
2. Voler vos informations confidentielles pour les réutiliser à leur profit (Carte Bancaire, codes d'accès Facebook…)
3. Voler vos documents (photos, documents d'entreprise, …)
4. Chantage en paralysant votre ordinateur et déblocage contre une somme d'argent (virement, achat forcé…)
5. Utiliser votre ordinateur pour déclencher des attaques : paralysie d'un serveur spécialement ciblé (déni de service) ou générateur de courriels (spam). Votre ordinateur infecté est appelé « zombie », intégré à un réseau (botnet ou réseau de robots) de plusieurs milliers d'autres ordinateurs infectés.

Technique :

1. Connexion à Internet avec un ordinateur ayant des failles de sécurité exploitables
2. Exécution d'un programme infecté

3. Ouverture d'une pièce jointe ou d'un document infecté
4. Navigation sur des sites douteux
5. Clic sur des bannières publicitaires infectées
6. Connexion de périphériques infectés (clef usb, disque dur amovible ...).

Les Bons réflexes :

Les malwares peuvent se propager par la technique du phishing par exemple. Les bons réflexes listés dans le chapitre phishing sont des réflexes qui marchent également pour les malwares. Les bons réflexes décrits dans le chapitre « ransomware » sont également à prendre compte.

En résumé, il faut :

1. Avoir un logiciel de sécurité (anti-virus) et le mettre à jour régulièrement
2. Faire des mises à jour régulièrement de votre système et de vos logiciels

Bon à savoir :

Les malwares ont plusieurs modes opératoires qui ont donné des noms comme :

1. Spyware ou « logiciel espion » en français, est un logiciel malveillant qui espionne votre activité et est chargé de récolter un maximum d'informations
2. Keylogger ou « enregistreur de frappe » en français, est un logiciel malveillant qui enregistre tout ce que vous pouvez taper sur votre clavier
3. Form-grabber ou « voleur de formulaire » en français, est un logiciel malveillant qui vole les informations que vous remplissez sur un formulaire
4. Trojan ou « Cheval de Troie » en français, est un malware qui se fait passer pour un logiciel légitime et qui exécute des actions malveillantes en arrière-plan
5. Worm ou « Ver informatique » en français, est un malware qui infecte votre ordinateur et s'auto-propage dans le système informatique pour infecter un maximum d'appareils électroniques sans l'action de l'attaquant
6. Backdoor ou « porte dérobée » en français, est un malware ou une fonction légitime installée par les éditeurs de logiciels afin d'avoir un accès direct à votre machine à votre insu

> Le phishing

Terme :
Le mot « phishing » vient de la phrase anglaise « password harvesting fishing » qui veut dire « pêche aux mots de passe ». En français, le terme est traduit par « filoutage » ou bien « hameçonnage ».

Objectif :
Le principe du phishing consiste à abuser de la crédulité des utilisateurs afin de voler des données personnelles comme les données bancaires, les identifiants/mots de passe etc.

Technique :
L'individu malveillant utilise d'abord la technique de l'usurpation d'identité afin de piéger l'utilisateur. Ici, l'usurpation d'identité passe par l'envoi d'un mail qui reprend la charte graphique d'un site dont l'individu malveillant a usurpé l'identité. L'attaquant malveillant reprend la charte graphique (graphisme, codes couleurs, formes etc.) d'une société ou bien d'une administration comme votre banque, la CAF, Impôts et bien d'autres afin de détourner votre attention.

L’individu malveillant peut utiliser, en même temps ou indépendamment, la technique de l’ingénierie sociale afin de vous piéger. L’ingénierie sociale consiste à récolter des informations sur vous sur les réseaux sociaux afin d’envoyer un message personnalisé à votre égard pour que vous tombiez plus facilement dans les mailles du filet de l’attaquant. Le mail contenant le message personnalisé s’appellera un « Spearphishing » en anglais ou « Hameçonnage ciblé » en français.

Une fois que vous recevez ce mail malveillant revêtant l’apparence d’un mail légitime venant d’une organisation privée ou publique « légitime » avec un message personnalisé ou non, on vous invite à cliquer sur un lien ou bien une pièce jointe. Souvent, le contenu du mail est à tendance alarmiste en vous disant que « votre compte sera bientôt fermé » ou bien « votre abonnement expire demain » etc. Tous ces messages sont là pour vous leurrer et causer du stress et/ou de l’inquiétude, afin que vous cliquiez sur ce fameux lien ou cette fameuse pièce jointe.

C’est ainsi, une fois que vous aurez cliqué sur le lien ou la pièce jointe, que vous communiquez vos données personnelles à l’attaquant car vous y êtes invités à le faire et donc le phishing a été réalisé avec succès du point de vue de l’individu malveillant.

<u>Les Bons Réflexes :</u>

1. Les mails faisant appel au phishing commencent souvent anonymement comme par exemple : « Cher/chère client(e) », « Madame, Monsieur » etc.

2. Vérifiez toujours l’émetteur du message avec son adresse mail et son nom. Si vous ne connaissez pas, ne cliquez pas dessus. De plus, l’adresse de l’émetteur d’un message (De :) est facilement usurpée car on peut y mettre ce que l’on veut.

3. Soyez méfiant des demandes (trop) urgentes d’informations personnelles, que ce soit par mail, appels téléphoniques, messages vocaux ou SMS.

4. Vérifiez le contenu du message qu’on vous a envoyé. S’il vous propose des choses qui sont trop belles pour être rêvées et/ou il y a des fautes d’orthographes, de grammaire, de syntaxe et/ou il y a des phrases en langue étrangère présentent dans le corps du mail alors que l’ensemble a été rédigé en français, cela veut dire que c’est malveillant.

5. Si tous les mails que vous avez reçu d’une personne, d’une société ou d’un organisme public ou privé étaient rédigés dans une langue et que d’un coup, un mail de cette même personne, société, organisme public ou privé est rédigé subitement dans une autre langue, sachez que cela doit être un message vérolé. Contactez votre interlocuteur par téléphone pour savoir si c’est bien l’émetteur du message.

6. Ne faites pas confiance aux informations personnelles contenues dans le mail. Elles ne cherchent qu’à le rendre légitime et ont pu être dérobées à votre insu.

7. Vérifiez l’URL en passant la souris sans cliquez dessus. Si l’URL indiquée est différente de celle habituelle, cela pourrait fort probablement signifier que c’est un lien malveillant

8. Si le message ou mail vous demande des informations personnelles comme mots de passe ou autre, sachez qu'en aucun cas quelqu'un doit vous les demander même si c'est une banque, les centres des impôts, CAF, mutuelles ou autres qui vous le demandent. Ce sont des informations personnelles et uniquement à usage personnel.

9. Ne cliquez sur une pièce jointe que si cela vient d'un émetteur de confiance.

10. Ne répondez jamais ou ne transférez jamais ce genre de mails à quelqu'un afin d'éviter de le contaminer

11. Utilisez les fonctions anti-phishing des navigateurs (Google Chrome, Internet Explorer, Mozilla Firefox, Safari), des logiciels de filtres « anti-pourriels »/« anti-spams » et des anti-virus récents. Cela va considérablement réduire les tentatives de phishing à votre encontre.

12. Vérifiez régulièrement les opérations effectuées sur vos comptes et votre carte bancaire

13. Au moindre doute, veuillez contacter la personne ou l'organisme qui vous a envoyé ce mail. Si vous avez cliqué par erreur et il s'est avéré que c'était une tentative de phishing, veuillez contacter votre cellule SSI.

14. De manière générale, soyez vigilant et faites preuve de bon sens.

Bon à savoir :

1. Le phishing se fait également par téléphone. Ce type de phishing s'appelle le « Vishing ». L'attaquant va utiliser un argumentaire très rôdé afin de vous soutirer des informations personnelles
2. Le phishing passe également par sms. Ce type de phishing s'appelle « Smishing ». L'attaquant va vous proposer de suivre un lien internet, d'appeler un numéro ou bien d'envoyer un sms.
3. La phishing peut aussi passer par la technique « fraude au président » (Whaling attack en anglais). C'est le fait de se faire passer pour le dirigeant ou une autre figure dirigeante de votre société afin de vous demander des informations confidentielles et sensibles. Ainsi, face à l'autorité, l'attaquant peut aisément avoir ce qu'il veut de vous.

> Le ransomware :

Terme :

Le ransomware ou bien « rançongiciel » en français est l'acronyme de deux mots qui sont « rançon » et « logiciel ». C'est tout simplement un type de logiciel malveillant.

Objectif :

Un ransomware a pour objectif de prendre en otage et de rendre indisponible l'accès à vos fichiers et vos données contenus dans vos appareils électroniques en les chiffrant. Le but étant ainsi de vous extorquer de l'argent, afin de récupérer vos données.

Technique :

Plusieurs techniques existent pour diffuser un ransomware sur vos appareils électroniques. Une des premières techniques est la diffusion par un mail malveillant. En effet, le ransomware utilise le phishing afin de contaminer vos appareils électroniques. Comme vous avez pu le voir précédemment, une fois que vous aurez cliqué dans le mail malveillant, le lien web ou bien la pièce jointe, le rançongiciel s'activera et se propagera dans votre système pour chiffrer vos données. Ainsi, vos données ne seront plus disponibles et pour les rendre à nouveau consultables, vous allez devoir payer une rançon pour obtenir la clé de déchiffrement. Nous vous invitons consulter le chapitre 1 sur le « phishing » afin de connaître plus en détails cette technique.

La deuxième technique pour propager un rançongiciel est de passer par le « malvertising ». Un « malvertising » est tout simplement de la publicité malveillante. Le fonctionnement est très simple, il s'agit d'utiliser des publicités en ligne afin de distribuer le rançongiciel dans votre système et il nécessite peu ou pas d'interactions avec l'utilisateur.

Le malvertising peut être présent sur des sites légitimes. Il se peut que pour être invisible aux yeux de l'utilisateur, le malvertising utilise un « iframe ». Un iframe est tout simplement un élément invisible dans la page web. Cet élément invisible vous renverra sur une page qui contient le fameux logiciel malveillant, « ransomware », sans vous rendre compte et ce dernier s'exécutera.

Les Bons réflexes :

Comme le ransomware se propage dans une de ces deux techniques via le phishing, nous vous invitons à regarder les bons réflexes autour du phishing dans le chapitre « phishing ». Ces bons réflexes ci-dessous sont à coupler avec ces derniers.

1. Ne payez jamais la rançon demandée par l'attaquant. En effet, vous ne ferez qu'alimenter son envie de continuer et de faire d'autres victimes. Appeler directement votre cellule SSI de votre entreprise et prévenez le CERT et SOC/SIEM de votre entreprise

2. Assurer vous de faire des sauvegardes régulières de vos données afin de les retrouver après l'incident. Sauvegardez-les sur un disque dur externe ou une clé USB afin d'avoir des sauvegardes qui ne sont pas connectées en ligne et pour ne pas les infecter.

3. Déconnectez également votre machine infectée d'Internet afin de stopper la propagation du virus et de couper le lien de communication entre le virus et le serveur distant qui le commande.

4. Assurez-vous que vos logiciels et votre système sont à jour afin d'avoir les derrières mises à jour de sécurité.

5. Assurez-vous également d'avoir un anti-virus

Bon à savoir :
Il existe 4 types de ransomware :

1. Le Scareware ou « alarmiciel » en français. C'est un type de rançongiciel qui revêt l'image d'un faux logiciel de sécurité ou d'un faux support technique. Une fenêtre s'ouvre subitement sur vote machine et vous prévient qu'un virus a été détecté ou autre chose et qu'il faut corriger cela en payant par exemple. Si vous ne répondez pas, vous continuerez sûrement à les recevoir.
   Sachez qu'un logiciel de sécurité légitime ne solliciterait jamais de cette façon son client. De même si vous n'avez pas installé ledit logiciel de sécurité, alors il est impossible qu'il ait pu détecter par hasard une infection.
2. Le Verrouilleur d'écran est un rançongiciel qui verrouille votre écran et la seule chose qui apparaisse, c'est une image soit disant « officielle » d'une organisation qui vous demande une rançon pour pouvoir à nouveau avoir accès.
3. Les ransomwares spécifique Mac existe également.
4. Les ransomwares sur mobiles existent aussi passant par des applications malveillantes par exemple

> Le spam

Terme :
Le mot spam est traduit par « pourriel » en français. Il désigne l'envoi de mails indésirables en grande quantité à des fins de publicité souvent. L'origine du mot vient d'un sketch comique qui fait référence à la marque de jambon « SPAM » qui est l'acronyme de « Spicy HAM ». Lors du sketch, la discussion autour de la marque SPAM a envahi toute la conversation et c'est ainsi, qu'il y a un parallèle avec le mot informatique « spam » car quand vous recevez des spams, cela envahit toute votre boîte mail.

Objectif :
1. Soit la vente d'un produit
2. Soit l'escroquerie
3. Soit infecter votre machine
4. Soit un canular
5. Soit faisant parti d'une campagne de phishing

Technique :
La technique utilisée ici est simplement l'envoi d'un mail directement sur votre machine. Il est souvent envoyé par un réseau de machines zombies ou « botnet » en anglais. Cela permet de rendre plus difficile la remontée de trace et l'envoi massif de courriel.

Les Bons réflexes :
Comme les spams se véhiculent par mails, les bons réflexes contenus dans le chapitre « phishing » sont à prendre en compte. Voici des mesures complémentaires également :

1. Activez l'option anti-spam de votre messagerie électronique
2. Désactivez l'option de téléchargement automatique des images dans les mails. En effet, souvent des malwares y sont cachés et si l'option est activée, le malware s'exécutera automatiquement

> Le scam

Terme :

Scam veut dire « arnaque ou ruse » en anglais.

Objectif :
Abuser de la crédulité des utilisateurs afin d'obtenir de l'argent en envoyant un mail, un sms ou un appel.

Technique :
Pour aboutir à un scam réussi, l'individu malveillant passe par l'envoi d'un mail ou d'un pourriel. Afin que vous tombiez dans le piège, plusieurs moyens sont utilisés telles que la compassion (il faut aider une personne par exemple), la crédulité (vous avez gagné une somme importante mais pour l'avoir, il faut verser des frais) ou le gain de cadeaux.

Les Bons réflexes :
Comme les scams passent par l'envoi de mails, les bons réflexes contenus dans le chapitre « phishing » sont à prendre en compte.

Bon à savoir :
D'autres formes d'arnaque cherchent à vous faire dépenser de l'argent en vous incitant à contacter des numéros surtaxés dont ils récupèrent une partie du profit :

1. Appel manqué : Votre téléphone portable sonne et le correspondant raccroche de suite. Le numéro affiché est, par exemple, +212 et autres indicateurs de pays étrangers ou pas. Vous allez chercher à contacter ce correspondant mystère en le rappelant et malheureusement, c'est un numéro surtaxé à l'appel et à la durée. Exemple : 1,35€ par appel plus 0,34 par minute.
2. SMS surtaxés : Vous recevez un SMS vous incitant à répondre. Quelques exemples :
   - « Bravo, vous avez gagné… Renvoyez GAIN au 54321 »,
   - « Votre compte est à découvert suite à un débit de 4768.58€… »,
   - « Votre carte de crédit a été utilisée pour des paiements suspects ».

   Le SMS vers ce numéro est surtaxé. ***Le bon réflexe*** : transmettez le SMS reçu au 33700. Le 33700 est un numéro court mis en place par l'association SMS+ dont les principaux opérateurs Français sont membres. Vous aurez plus d'informations sur leur site « http://www.33700-spam-sms.fr/ ».

> Ingénierie sociale

Terme :
Ingénierie sociale ou en anglais « Social Engineering » est un des moyens pour parvenir à réaliser les différentes attaques informatiques que vous avez vues ci-dessus.

Objectif :
Parvenir à voler des informations personnelles de la victime afin de commettre des attaques informatiques contre cette dernière ou contre l'organisation pour qui elle travaille. En outre, l'appât du gain financier est un des objectifs également de l'ingénierie sociale.

Technique :

C’est un des moyens « informatiques » les plus simples à réaliser. Comme c’est une technique qui se base sur la faille humaine, les chances de réussites sont données à tout le monde. En effet, il s’agit simplement de trouver toutes les informations disponibles sur internet et les réseaux sociaux sur votre victime et les exploiter afin de manipuler cette dernière.

Les bons réflexes :

Comme pour toutes les autres attaques informatiques que nous avons vues ci-dessus, certains réflexes sont à adopter comme :

1. Naviguez sur des sites internet officiels et sécurisés (site en https ayant un cadenas ou une clé également sur la barre du navigateur)
2. Utilisez des applications officielles
3. Mettez à jour votre navigateur internet ainsi que tous vos appareils électroniques : ordinateurs, téléphones, tablettes etc.
4. Configurez vos comptes de vos réseaux sociaux et autres sites internet afin d’être plus sécurisé
5. Partagez seulement les informations (photos, statuts, etc.) nécessaires et utiles sur internet et les réseaux sociaux
6. Faites attention aux invitations ou propositions que vous recevez
7. Faites attention à l’utilisation des réseaux sociaux en entreprise au risque de contaminer cette dernière sans vous rendre compte
8. Utilisez des mots de passe robustes et différents pour chaque compte, site internet, application, etc., afin de diminuer les chances de l’attaquant de les trouver

Best practices
Anti-Fraud & Information Security

> ANTI-FRAUD

Every day you carry out banking transactions through several technological means or not, such as internet, telephone, in bank branches or by the different online payments. However, you inevitably increase the risk of bank fraud by using all these services at your disposal. Thus, these operations require simple and effective measures in order to carry them out in good safety conditions.

Societe Generale Factoring ensures that you have a high level of security so that you can navigate into your accounts and carry out banking transactions safely.

As a customer, you are the first actor in the protection of your personal and banking data. Therefore, it is important to know the different fraud risks through different examples of cyber-attacks in the following chapter (Information Security) in order to prevent them. Please note that no bank or other private or public organizations will ask you by phone or email for your personal data such as credit card codes, passwords, credentials etc. because there are confidential data of which you are the single owner.

In case of doubt, please contact SG Factoring via the official number (and not the telephone number in the email you received in case) to request the veracity of this request, in order to prevent you from experiencing potential fraud against you.

If you think, you have been victim of fraud, please contact SG Factoring and please file a complaint with the police also.

Banking information:
All of your single-use codes, passwords and credentials used, either to connect to your customer accounts or to perform transactions on your bank's website or application, are confidential and sensitive. Thus, they should never be disclosed to anyone in order to avoid bank fraud. Unless using them on the bank's website or app.

All information related to your bank account, credit card are also sensitive and confidential and must be protected against fraud attempts.

Personal data:
Your personal data are also elements to protect against the risk of fraud because associated with banking data, malicious individuals will use them in order to commit different types of cyber-attacks. These personal data are for example:

- Name and last name
- Postal address
- Date of birth
- Telephone number
- E-mail address

How can we protect them?
Multiple measures need to be followed in order to protect them and to avoid fraud carried out by malicious individuals:

1. Avoid writing on paper your access codes, credit card numbers or any others credentials
2. Refuse to memorize passwords on website
3. Never communicate banking or personal information such as bank numbers, email or phone numbers to an unidentified third party or whose reputation is not secure
4. Only communicate your banking data on reliable sites and through secure communications (https)
5. Avoid sending your banking data by email and instant messaging
6. Notify your bank immediately of any illegitimate changes to your personal information
7. Regularly delete temporary cookies and Internet files from your computer

> INFORMATION SECURITY

> Malwares

Definition:
Malware comes from the word “malicious software”. You will often hear the word “virus” used to refer to malware, but it is a definition that is misused. This comes from the fact that the first malware was a virus.

Objective:

1. Sell a product by recording your Internet browsing to better target your habits
2. Steal your confidential information to reuse for their benefit (Credit Card, Facebook access codes…)
3. Steal your documents (photos, corporate documents …)
4. Blackmail by paralyzing your computer and unlocking it for money (transfer, forced purchase…)
5. Use your computer to trigger attacks: paralyzing a specific targeted server (denial of service) or spamming you. Your infected computer is called «zombie», embedded in a network (botnet) of thousands of other infected computers.

Technique:
Several techniques are used to propagate malwares:

1. Internet connection with a computer which has exploitable security vulnerabilities
2. Running an infected program
3. Opening an infected attachment or document
4. Navigating on suspicious web-sites
5. Clicking on infected banner ads
6. Connecting on infected devices (usb key, removable hard drive ...).

Best practices:
Malwares can be spread by phishing, for example. The best practices listed in the phishing chapter also work for malwares. Those described in the «ransomware» chapter are also to be taken into account. In short, it is necessary to:

1. Have security software (anti-virus) and update it regularly
2. Update your system and software regularly

Good to know:
The malwares have several operating modes that have given names like :

1. Spyware, which is a malicious software that spies your activity and collects as much information as possible
2. Keylogger, which is a malicious software that records everything you can type on your keyboard
3. Form-grabber or form thief, is a malicious software that steals the information you fill out on a form
4. Trojan, which is a malware that pretends to be legitimate software and executes malicious actions in the background
5. Worm, which is a malware that infects your computer and self-propagates in the computer system to infect a maximum of electronic devices without the action of the attacker
6. Backdoor, which is a malware or a legitimate function installed by software publishers in order to have direct access to your machine without your knowledge

> Phishing

Definition:
The word “phishing” comes from the sentence “password harvesting fishing”.

Objective:
The phishing attack consists in abusing user’s credulity in order to steal personal data such as banking data, credentials etc.

Technique:
The malicious individual first uses the identity theft technique to trap the user. Here, identity theft involves sending an e-mail that takes over the graphic design of a site whose identity was stolen by the malicious individual. The malicious attacker uses a company’s graphic chart (graphics, color codes, shapes, etc.) such as your bank and many others private or public organizations to deflect your attention.

The malicious individual can use, at the same time or independently, the social engineering technique to trap you. Social engineering is about gathering information about you on social networks in order to send you a personalized message so that you can more easily be trapped through the cracks of the attacker’s net. The email containing the personalized message will be called a “Spearphishing”.

Once you receive this malicious mail in the appearance of a legitimate email from a private or public organization with a personalized message or not, you are invited to click on a link or an attachment. Often, the content of the mail is alarmist by telling you that

«your account will soon be closed» or «your subscription expires tomorrow» etc. All these messages are there to lure you and cause stress and/or worries through these messages so that you click on that famous link or attachment.

This is so, once you have clicked on the link or attachment, that you communicate your personal data to the attacker as you are invited to do so and therefore phishing has been successfully achieved.

Best practices:

1. Phishing emails often start anonymously, such as “Dear Customer”, “Dear Sir”, etc.

2. Always check the sender of the message with its email address and name. If you do not know, do not click on it. In addition, the address of the sender of a message (From:) is easily usurped because you can put what you want in it.

3. Be wary of urgent requests for personal information, whether by email, phone calls, voice messages or SMS.

4. Check the content of the message sent to you. If it offers you things that are too beautiful to be dreamed of and/or there are grammar, syntax errors and/or foreign language sentences present in the body of the mail while the whole was written in English, that means it’s malicious

5. If all the e-mails you received from a person, company or public or private organizations were written in one language and suddenly an e-mail from that same person, company, public or private organization, is written suddenly in another language, we want you to know that this must be a malicious e-mail. Contact the person by phone to find out if he/she is the sender of the message.

6. Do not trust the personal information contained in the email. They only seek to make the email legitimate and may have been stolen without your knowledge.

7. Check the URL by hovering the mouse without clicking on it. If it indicates you something else than the usual URL, it probably means it’s a malicious link.

8. If the message or email asks you for personal information like passwords for example, you need to know that in no case should someone ask you this even if it is a bank, tax centers or others. This is personal information and only for personal use.

9. Only click on an attachment if it comes from a trusted issuer.

10. Never answer or forward such emails to anyone to avoid contaminating them.

11. Use the anti-phishing features of browsers (Google Chrome, Internet Explorer, Mozilla Firefox, Safari), anti-spam filter software and recent anti-viruses. This will dramatically reduce phishing attempts against you

12. Check your bank card and account transactions regularly

13. In case of doubt, please contact the person or organization that sent you this email. If you clicked by mistake and it turned out that it was a phishing attempt, please contact your Security team

14. In general, be vigilant and use common sense.

Good to know:

1. Phishing is also done by telephone. This type of phishing is called **"Vishing".** The attacker will use a very sophisticated argument to extract your personal information
2. Phishing also goes through messages. This type of phishing is called **"Smishing".** The attacker will propose you to follow an internet link, call a number or send a text.
3. Phishing can also be done using the **Whaling attack**. It is the act of pretending to be the CEO or another Managing Director of your company in order to ask you for confidential and sensitive information.

> Ransomware

Definition:
Ransomware is the acronym of two words which are "ransom" and "software".

Objective:
A ransomware aims to hold hostage and make unavailable the access to your files and data contained in your electronic devices by encrypting them. The goal is to extort money by asking you to pay the ransom, in order to recover the data.

Technique:
Several techniques exist to spread ransomware to your electronic devices. The first technique is by a malicious mail. Indeed, ransomware uses phishing to contaminate your electronic devices. As you may have seen earlier, once you have clicked in the malicious mail, web link or attachment, the ransomware will be activated and propagated in your system to encrypt your data. Thus, your data will no longer be available and to make them available again, you will have to pay a ransom to get the decryption key. We invite you to see chapter 1 on "phishing" to learn more about this technique.

The second technique to propagate a ransomware is to go through the "malvertising". Malvertising is a malicious advertising. It involves using online advertisements in order to spread the ransomware in your system and it requires little or no interaction with the user.
Malvertising may be present on legitimate sites. To be invisible to the user, malvertising may use an iframe. An iframe is simply an invisible element in the web page. This invisible element will return you to a page containing the famous «ransomware» without noticing it and it will run.

Best practices:
As ransomware is propagated also via phishing as we seen it previously, we invite you to look at the best practices around phishing in the «phishing» chapter. Those below are to be coupled with these.

1. Never pay the ransom requested by the attacker. Indeed, you will only fuel his desire to continue and make other victims. Call your company's security team unit directly and notify your company's CERT and SOC/SIEM
2. Ensure that you make regular backups of your data to retrieve them after the incident. Save them to an external hard drive or USB drive to have backups that are not connected online and not infect them
3. Also disconnect your infected machine from the Internet to stop the spread of the virus and cut the communication link between the virus and the remote server that controls it.
4. Ensure that your software and system are up-to-date in order to have the last security updates.
5. Also make sure you have an anti-virus

Good to know:
There are 4 more types of ransomware which are :

1. Scareware, which is a type of ransomware that show you a fake image of a false security software or a false technical support. A window suddenly opens on your machine and warns you that a virus has been detected or something else and that you must correct this by paying for example. If you do not respond, you will surely continue to receive them.
   Be aware that legitimate security software would never solicit its client in this way.
2. The Screen Lock, which is a ransomware that locks your screen and the only thing that appears is a so-called "official" image of an organization that asks you to pay a ransom to be able to access it again
3. Mac specific ransomware also exists.
4. Mobile ransomware also exists through malicious applications for example

> Spam

Definition:
It refers to sending unwanted emails in high volume, often for advertising purposes. The origin of the word comes from a comic sketch that refers to the brand of ham "SPAM" which is the acronym of "Spicy HAM". During the sketch, the discussion around the SPAM brand invaded the whole conversation and so, "spam' in IT refers to that.

Objective:
Several objectives are present in spam which are for example,

1. The sale of a product
2. The scam
3. Infect your machine
4. Be a hoax
5. Doing a phishing campaign

Technique:
The technique used here, is sending an email directly to your machine. It is often sent by a network of zombie machines or "botnet".

Best practices:
As spam is spread by mail, the best practices contained in the «phishing» chapter must be taken into account. Additional measures include:

1. Enable the anti-spam option in your email
2. Disable the option to automatically upload images to emails. Indeed, often malwares are hidden in it and if activated, it will run automatically.

> Scams

Definition:
Scam means “ruse”.

Objective:
Abusing the credulity of users to get money by sending an email, text or call.

Technique:
To achieve a successful scam, the malicious individual sends an email or spam. In order to trap you, several means are used either by compassion (you have to help a person for example), credulity (you have earned a large sum but to have it you have to pay a fee) or the gift gain.

Best practices:
As scams go through mails, in most cases, the best practices contained in the «phishing» chapter are to be taken into account.

Good to know:
Other forms of scams seek to make you spend money by encouraging you to contact high-tax numbers from which they recover part of the profit:

1. **Missed call**: Your phone rings and the caller hangs up. The number displayed is 0899… You will try to contact this mystery correspondent and unfortunately, it is a number overtaxed on call and duration. Example: €1.35 per call plus 0.34 per minute
2. **Overtaxed Messages**: You receive a message prompting you to respond. Some examples:
   “Congrats, you won… Return WIN to 54321”,
   “Your account is overdrawn following a debit of €4768.58…”,
   “Your credit card was used for suspicious payments”.
   The message to this number is overtaxed.

> Social Engineering

Definition:

Social Engineering is one of the ways to achieve the various cyber-attacks you have seen above.

Objective :

Stealing personal data from the victim in order to commit cyber-attacks against the latter or against the organization for which it works. In addition, the lure of financial gain is also one of the objectives of social engineering

Technique:

It is one of the simplest “cyber-attack” to achieve. As it is a technique based on the human failure, the chances of success are given to everyone. Indeed, it is simply a

matter of finding all the information you can on the internet and social networks about your victim and exploiting it in order to manipulate it.

Best practices:

As with all the other cyber-attacks we have seen above, some practices are to be adopted, such as:

1) Browse official and secure websites (https site with a lock or key also on the browser bar)
2) Use official applications
3) Update your internet browser and all your electronic devices: computers, phones, tablets etc.
4) Set up your accounts on your social networks and other websites to be more secure
5) Share only the necessary and useful information (photos, status, etc.) on the internet and social networks
6) Pay attention to invitations or proposals you receive
7) Pay attention to the use of social networks at work at the risk of contaminating your company's network without realizing
8) Use robust and different passwords for each account, website, application, etc., in order to reduce the attacker's opportunities of finding them