CYBERMOI/S 2023

Un mois pour devenir #CyberResponsable

CYBER MOIS X SYNOVO GROUP
IT & SOFTWARE SOLUTIONS

Edito

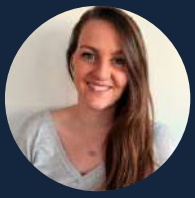
A l'occasion du Cybermoi/s 2023, Synovo Group a réuni ses experts pour échanger et élaborer ce livret autour de la thématique choisie par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) : **la fraude par ingénierie sociale**. Retrouvez leurs meilleurs conseils et astuces pour vous protéger en ligne, que vous soyez professionnel ou particulier !

Ce qui a été élaboré avec nos experts et témoins :

Michel L.
Dirigeant

Guillaume P.
Dirigeant

Romain C.
Responsable de la Sécurité des Systèmes d'Information



Lisa C.
Responsable Marketing et Communication

CYBERMOI/S 2023

Sommaire

INGÉNIERIE SOCIALE

Qu'est-ce que c'est ?

DÉFINITION

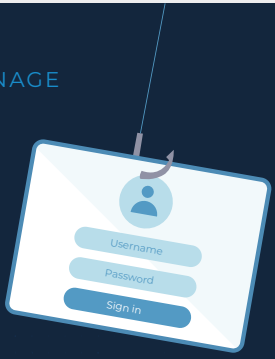
Ingénierie sociale

L'ingénierie sociale est une technique qui vise à manipuler les individus pour obtenir des informations confidentielles ou les amener à accomplir des actions spécifiques à des fins malveillantes. Elle repose principalement sur la manipulation psychologique plutôt que sur l'exploitation de failles techniques.

La forme la plus répandue d'attaques par ingénierie sociale est le *phishing*.

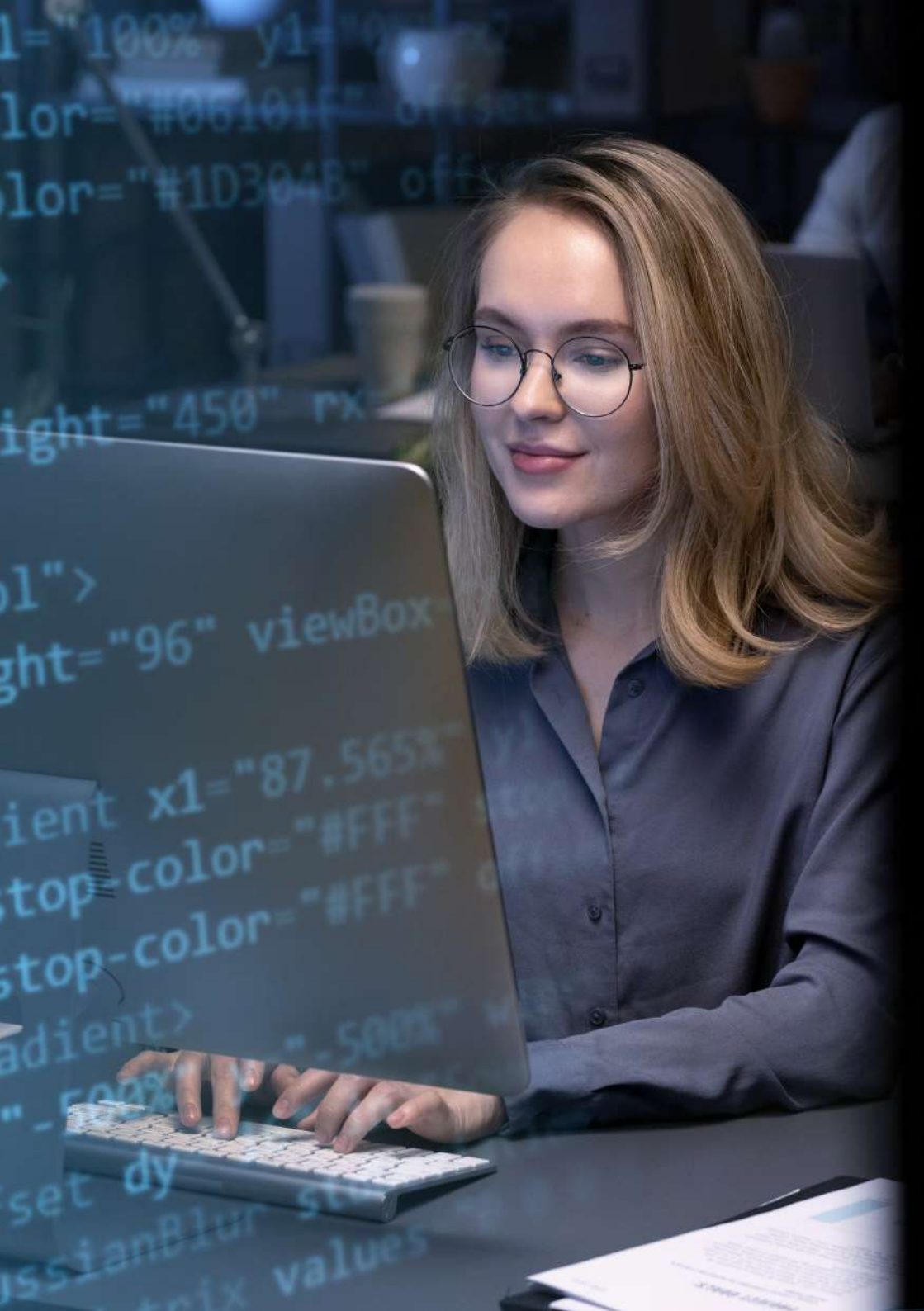
FOCUS *PHISHING*, OU HAMEÇONNAGE

Le *phishing*, ou hameçonnage, est une forme d'escroquerie en ligne où le fraudeur / cybercriminel se fait passer pour une entité de confiance (banque, service des impôts, proche, etc.) dans le but de voler des informations personnelles et sensibles telles que des mots de passe, des numéros de comptes, numéros de cartes de crédit ou autres informations généralement financières.



Les cas de *phishing* se sont multipliés au cours des dernières années.
Il s'agit aujourd'hui d'une attaque courante et très répandue pour plusieurs raisons : facilité d'exécution, diversification des modes opératoires, développement de la manipulation psychologique en ligne, exploitation d'un sentiment d'urgence ou encore le manque de sensibilisation des personnes.

Il existe plusieurs types d'arnaques à l'hameçonnage : les emails de hameçonnage en masse, le hameçonnage vocal par téléphone (*vishing*), le hameçonnage par SMS (*smishing*), le hameçonnage sur les réseaux sociaux (*angler phishing*), le hameçonnage par QR Code (*quishing*), le harponnage...



ATTAQUES PAR INGÉNIERIE SOCIALE

Découvrez les témoignages et les conseils de nos experts

TÉMOIGNAGE 1

Fausse annonce de location

« En réponse à une annonce de location sur Leboncoin, une personne de mon entourage a envoyé un dossier de candidature complet avec les informations du futur locataire prétendu ainsi que des différents garants.

L'annonce de location était en réalité complètement fausse : le but était simplement de récupérer suffisamment d'informations personnelles et financières afin d'ouvrir un crédit à la consommation de 4000€ !

Heureusement, elle a pu être remboursée grâce à une micro-inattention de la société de crédit qui a reconnu ne pas avoir eu l'authentique carte d'identité. »

\- Guillaume P.

LE MOT DES EXPERTS

Il s'agit ici d'un exemple typique d'ingénierie sociale et d'abus de confiance : le prétendu propriétaire a joué sur la compétitivité de l'annonce et déclaré que le premier dossier rempli aurait l'appartement. C'est une forme d'urgence très répandue. Comme bien souvent, les cyberattaques ont objectif d'extorquer de l'argent à un tiers, que ce soit une société ou un particulier.

QUE FAIRE DANS CE GENRE DE SITUATION ?

Si vous êtes confronté à une telle annonce, vous ne pouvez jamais être sûr de l'authenticité de celle-ci.

Ne donnez JAMAIS L'ORIGINAL de vos documents, et ajoutez si possible la mention « duplicata ».

Si jamais vous êtes victime d'une telle attaque, prévenez immédiatement votre banque, la société de crédits à la consommation et votre assurance.


facebook.com
facebook
Get Facebook for iPhone and browse faster
Mobile number or email
Password
Log In
or
Create New Account
Forgot Password?

TÉMOIGNAGE 2

Harponnage sur Messenger

« Mon amie a cliqué sur le lien du message pour voir la photo en question. Elle a été redirigée sur une page de connexion à Facebook.

Rien n'indiquait une arnaque, voir la photo sur Facebook lui paraissait logique puisque le message venait de Messenger. Elle a entré son identifiant et son mot de passe. C'est à ce moment qu'elle a compris que c'était une attaque : le même message qu'elle avait reçu a été envoyé à tous ses amis (sa base de données) !

Heureusement, elle a réagit rapidement en publiant une annonce pour prévenir ses amis et éviter de propager l'arnaque. Evidemment, elle a changé tous ses mots de passe. »

\- Lisa C.

LE MOT DE L'EXPERT

En réalité, la version en ligne de Facebook sur laquelle la personne a renseigné ses informations était un clonage de site web : le cybercriminel a créé une page internet ressemblant à celle de Facebook comme leurre, et les informations renseignées par les victimes quand elles pensaient se connecter lui était envoyées par mail. Ainsi, avec l'identifiant et le mot de passe de chacun, le pirate pouvait dupliquer son message.

Pourquoi récupérer des codes d'accès Facebook ?

Car bien souvent, les particuliers non sensibilisés à la cybersécurité possèdent les mêmes identifiants partout : réseaux sociaux certes, mais aussi applications mails, bancaires, etc. Si les codes sont les mêmes partout, des pertes financières peuvent alors être très conséquentes !

QUE FAIRE DANS CE GENRE DE SITUATION ?

Changez IMMÉDIATEMENT tous vos mots de passe (réseaux sociaux, applications bancaires, comptes d'assurances, etc.) et alertez votre entourage susceptible d'être également victime de l'attaque.


VPN
VPN

TÉMOIGNAGE 3

Du *phishing* au cyber-chantage

« En tant que RSSI, je me dois d'être informé des différentes attaques qui peuvent toucher les professionnels et les entreprises.

J'ai notamment été marqué par l'attaque ayant touché la société Uber en septembre 2022. Un jeune homme d'à peine 18 ans est parvenu à pirater tout le système d'information d'Uber ! En se faisant passer pour un collaborateur du service informatique, il a envoyé des mails à plusieurs employés leur demandant de réinitialiser leurs identifiants et mots de passe au VPN.

Il a utilisé les codes obtenus pour hacker le système et faire chanter Uber en menaçant de divulguer toutes les données récoltées. »

- Romain C.

LE MOT DES EXPERTS

Le *phishing* par mail est le plus répandu. Couplé à un manque de sensibilisation du personnel, il devient très facile pour les cybercriminels d'accéder à des données sensibles.
En tant que professionnel, quelle que soit l'échelle et le secteur, il est important de sensibiliser ses collaborateurs aux différentes formes de *phishing* afin qu'ils puissent reconnaître les mails frauduleux, par exemple. Cela évite la fuite et / ou le vol de données, le chantage, les demandes de rançons, etc.

Il existe également des procédures à mettre en place et des certifications à obtenir pour prévenir de telles attaques. Par exemple, Synovo Group est certifié ISO 27001 et Hébergeur de Données de Santé (HDS) pour garantir à ses clients l'hébergement de leurs logiciels et de leurs données le plus sécurisé possible !

QUE FAIRE DANS CE GENRE DE SITUATION ?

Si vous êtes victime de cyber-chantage (blocage de votre appareil, divulgation de photographies sensibles, fuite de données personnelles, etc.), surtout ne payez pas ! La plupart du temps, la menace n'est pas réelle.

Par ailleurs, si vous concédez à payer une fois, le pirate reviendra de façon de plus en plus régulière et avec des montants de plus en plus importants. Vous pouvez également aller voir la police pour signaler l'attaque si vous craignez réellement la menace.

COMMENT SE PROTÉGER DU *PHISHING* ?

Romain vous dévoile les bonnes habitudes à avoir

A l'ère du digital et avec l'avènement du télétravail, les techniques de *phishing* se sont multipliées et donc perfectionnées. Elles sont de plus en plus réalistes. Heureusement, il existe toujours des failles que vous pouvez exploiter et des habitudes à mettre en place pour vous protéger.

Vérifier l'adresse mail et le nom de domaine

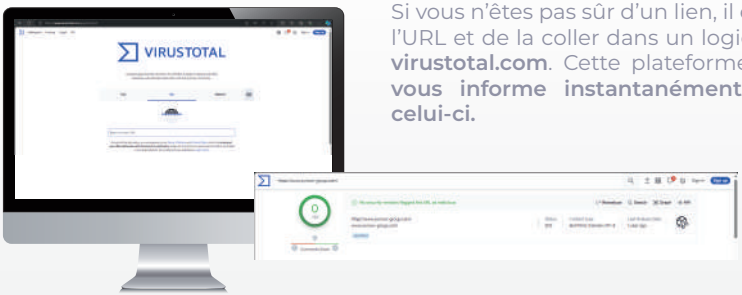
Lorsque vous recevez un courriel, **vérifiez toujours l'adresse mail de l'expéditeur**. La plupart du temps, le nom sera mal orthographié (parfois à *une lettre* près).

Vous pouvez également **analyser le nom de domaine** (la partie qui se trouve après l'arobase : @**entreprise.com**, par exemple). Au sein d'une même entreprise, le nom de domaine est généralement toujours le même. Si vous avez déjà reçu un mail d'une personne venant de la même société, comparez les noms de domaine pour voir s'ils sont identiques.

Se méfier des liens

Il existe différentes méthodes simples pour s'assurer que les liens disponibles sont fiables. Si le lien est intégré dans un mot ou un groupe de mots (par exemple, via un bouton « *Inscrivez-vous* »), il suffit de **passer la souris sur l'entité cliquable**. Le véritable lien apparaitra alors et vous pourrez le lire.

Il est aussi possible que le lien soit écrit dans le corps du texte, mais qu'**il diffère du lien de redirection** ! Prenez toujours en compte le lien qui apparait avec votre souris.



Si vous n'êtes pas sûr d'un lien, il est possible de copier l'URL et de la coller dans un logiciel d'analyse, tel que **virustotal.com**. Cette plateforme **examine le lien et vous informe instantanément de la fiabilité de celui-ci.**

Utiliser les messageries internes aux applications

Si vous recevez un mail de votre banque sur votre messagerie personnelle, ne l'ouvrez pas. **Rendez-vous directement sur votre application bancaire**, puis dans l'onglet messagerie. Si le message est important et réel, il y figurera également. Si vous ne voyez rien, c'est qu'il s'agit d'une tentative de *phishing* !

Contacter l'expéditeur via un autre canal

Si vous recevez un mail qui vous semble suspect, n'hésitez pas à **contacter le prétendu expéditeur via un autre canal** (appel téléphonique, message privé, etc.). Il vous confirmera ou infirmera la légitimité du mail.

Bien entendu, vous pouvez simplement ignorer le mail douteux. Si le message est réellement important, la personne vous recontactera elle-même par téléphone pour vous notifier l'information.

Ne jamais envoyer d'original

Peu importe le contexte ou la personne, il est primordial de ne jamais envoyer d'original de vos documents (RIB, carte d'identité, déclaration d'impôts, etc.). Faites des photocopies sur lesquelles vous ajoutez la mention « *duplicata pour telle utilisation* ». Ainsi, vos documents ne pourront pas être utilisés à d'autres fins frauduleuses.

Eviter de communiquer des informations personnelles sur les réseaux

Limitez autant que possible de communiquer des informations personnelles en ligne : membres de la famille, collègues, trajets quotidiens, lieu de travail, etc. Toutes ces informations permettent aux pirates de mieux usurper votre identité auprès de votre cercle : il devient très facile de se faire passer pour vous !

Utiliser des mots de passe différents

On ne le dira jamais assez : générer des mots de passe différents pour chaque plateforme et application est l'une des meilleures façons de se protéger. En effet, **posséder des mots de passe complexes et uniques limite les risques d'attaques** : ils sont très difficiles à craquer et ne pourront servir qu'une fois / sur une seule plateforme.

Conscient que vous pouvez avoir de nombreux mots de passe et qu'il peut être difficile de tous les retenir, voici quelques astuces pour vous simplifier la tâche :

- Utilisez la fonctionnalité « *mémoriser le mot de passe* » de votre navigateur *web* : il vous les rappellera automatiquement à chaque connexion sur votre propre appareil

- Téléchargez un logiciel sécurisé dans lequel vous pourrez enregistrer tous vos mots de passe, ainsi vous n'aurez qu'à retenir l'identifiant et le mot de passe de votre session

Se renseigner et sensibiliser son entourage

Il existe de nombreuses entités de sensibilisation à la cybersécurité : l'**ANSSI**, **cybermalveillance.gouv.fr**, la **Commission Nationale de l'Informatique et des Libertés (CNIL)**, etc. N'hésitez pas à consulter leurs sites internet et les ressources qu'elles mettent à disposition pour vous informer sur le sujet.

Vous pouvez également **en parler à votre entourage et partager des conseils à vos proches**. Plus il y a de personnes averties, moins les attaques seront efficaces !


CYBER
MOIs
X
SYNOVO GROUP
IT & SOFTWARE SOLUTIONS