PARLONS CYBER SÉCURITÉ

AVEC SYLVAIN CALLOT, LIONEL RAUCH ET LAURENT VERDIER

WEBINAIRE ORGANISÉ PAR GRANNY GEEK

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CONSEILLER NUMÉRIQUE
France services

Financé par
GOUVERNEMENT
Liberté
Égalité
Fraternité

FRANCE RELANCE

Financé par l'Union européenne
NextGenerationEU

GRANNY GEEK
TOUS AU NUMEREEK

GRANNY GEEK®

SUITE À CETTE VISIO

Vous pourrez :

- Améliorer les compétences de vos bénéficiaires (vigilance, technique, communication).

- Apaiser vos apprenants et les rassurer sur leurs capacités et leurs compétences.

- Rendre le sujet de la cybersécurité plus compréhensible pour les apprenants.

GRANNY GEEK®

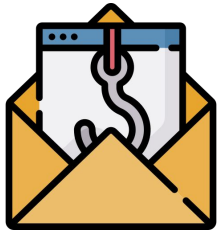
SOMMAIRE

- Quelques chiffres
- Mots de passe
- Phishing, Sms, Qr code...
- Virus, Faux support technique
- Recommandations
- Questions / Réponses

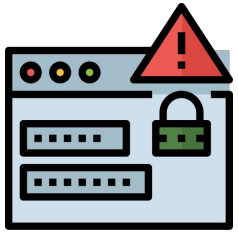
DÉFINITION

LES DIFFÉRENTS TYPES D'ARNAQUES

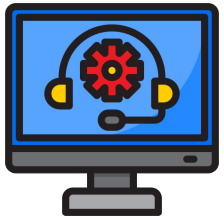
E-MAILS, SMS : Phishing, hameçonnage... (31%)



> E-mail d'un proche en difficulté (Ami, connaissance...)
> Gains, cadeaux, promotions
> Accès à un service arrêté (banques, administrations...)
> Problème de sécurité, livraison, factures (FAI, La poste...)
> Infraction, message d'interpole, de la gendarmerie
> CPF, accès à un compte
> Vignettes Crit'air, carte vitale



PIRATAGE D'UN COMPTE : (19%)



> Compte e-mail, comptes utilisateurs

FAUX SUPPORT TECHNIQUE: (13%)

> Écran bleu avec un son strident
> Message que votre ordinateur est infecté avec N° gratuit

Les ressources du GIP Cyber malveillance : les différents types de piratage informatique.

DÉFINITION

QUELQUES NOTIONS À CONNAÎTRE

PRIX D'UN SERVICE SUR LE MARCHÉ DE L'ARNAQUE :

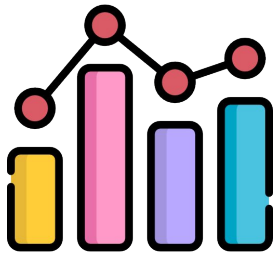
> 200€ pour des identifiants de paiement
> 1€ pour un numéro de sécurité sociale
> 10€ pour des identifiants de service de streaming
> 110€ pour un numéro de carte bancaire
> 2000€ pour un passeport
> 1000€ pour des dossiers médicaux

MOTIVATION :

> Argent, vol de propriété, espionnage

QUELQUES CHIFFRES :

> 38% d'attaques en plus entre 2021 et 2022
> 94% des logiciels malveillants sont délivrés par mail



Données : Afnor, Check Point Research

SÉCURITÉ

QU'EST-CE QU'UN MOT DE PASSE FAIBLE ?

En 2022, un mot de passe faible est :

- Un mot de passe de moins de 12 caractères
- Ne contient qu'une suite de caractères identiques (chiffres ou lettres)
- Contient des informations personnelles (date de naissance, code postal, nom de votre animal...)
- Une suite de caractères du clavier

Quelques exemples des pires mots de passe :

- 123456
- 1234561
- 123456789
- Azerty
- Azerty12345
- Azertyuiop
- Wxcvbn
- doudou
- chouchou
- motdepasse
- password
- incorrect
- 000000
- marseille
- qwerty
- loulou
- utilisateur
- password
- paris
- spiderman
- superman

Les ressources du GIP Cyber malveillance : les mots de passe.

SÉCURITÉ

QU'EST-CE QU'UN MOT DE PASSE FAIBLE ?

Temps de piratage d'un mot de passe en 2023

Nombre de caractères	Chiffres	Minuscules	Minuscules + Majuscules	Chiffres + Minuscules + Majuscules	Chiffres + Minuscules + Majuscules + caractères spéciaux
4	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
5	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
6	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
7	Instantanément	Instantanément	1 secs	2 secs	4 secs
8	Instantanément	Instantanément	28 secs	2 mins	5 mins
9	Instantanément	3 secs	24 mins	2 h	6 h
10	Instantanément	1 mins	21 h	5 jours	2 semaines
11	Instantanément	32 mins	1 mois	10 mois	3 ans
12	1 secs	14 h	6 ans	53 ans	226 ans
13	5 secs	2 semaines	332 ans	3 000 ans	15 000 ans
14	52 secs	1 an	17 000 ans	202 000 ans	1 million ans
15	9 mins	27 ans	898 000 ans	12 millions ans	77 millions ans
16	1 h	713 ans	46 millions ans	779 millions ans	5 milliards ans
17	14 h	18 000 ans	2 milliards ans	48 milliards ans	380 milliards ans
18	6 jours	481 000 ans	126 milliards ans	1 000 milliards ans	26 000 milliards ans

Vérifier les mots de passe

France Num : Combien de temps un pirate met-il pour trouver votre mot de passe ? Comment vous protéger ?

HAMEÇONNAGE

COMMENT S'EN PRÉMUNIR ?

LA PRÉVENTION :

> Personne ne peut connaître l'ensemble des attaques

> Il existe des critères pour éviter de se faire avoir :

- Vérifier les liens quand c'est possible (sur ordinateur).
- Se renseigner directement à la source (banque, ami(e)s...)
- Repérer les fautes ou choses suspectes.
- Supprimer les mails suspects et vider la corbeille.

> Faire le parallèle avec des évènements courants (courriers de pub, gains d'argent...)

Les ressources du GIP Cyber malveillance : reconnaître un mail de phishing ou d'hameçonnage.

HAMEÇONNAGE

COMMENT RÉAGIR

SI VOS BÉNÉFICIAIRES ONT RÉPONDU À UNE ARNAQUE EN LIGNE :

> Donner les conseils de premières urgences.

> Rassurer sur les procédures et les accompagner.

> Des solutions existent :
- L'opposition bancaire
- Les solutions techniques (analyses antivirus, antimalware, nettoyeurs)
- Assistance des plateformes, accompagnement d'associations...

PIRATAGE

CONSEILS ET ACCOMPAGNEMENTS

EN PRÉVENTION :

> Expliquer les mots de passe (pourquoi, comment...)
- Pourquoi créer des mots de passe complexes.
- Comment les modifier régulièrement.
- Comment utiliser un gestionnaire de mots de passe.
- Pourquoi ajouter un numéro de téléphone.

> Améliorer la sécurité (double authentification, mail de récupération...)

> Faire des sauvegardes régulières.

> Donner les procédures, des conseils de navigation sur internet...

PIRATAGE

COMMENT Y RÉPONDRE

EN CAS DE PIRATAGE :

> Qui avertir et comment
- Le service sur lequel est le compte (FAI, administration).
- Les proches.

> Les solutions existent :
- Modification du mot de passe.
- Récupérer son compte.
- Analyser son support.
- Analyser la sécurité des mots de passe.

> Préparer une check-list des procédures.

FAUX SUPPORT

AVERTIR

LA PRÉVENTION :

> Prévenir et faire le parallèle avec la vie courante.

> Comment cela arrive :
- Ce blocage n'intervient que lors de la navigation sur internet.

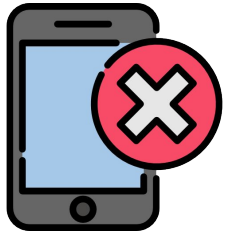
> Eviter les blocages par des solutions techniques et explication du fonctionnement :
- Extension de sécurité sur les navigateurs.
- Bloqueurs de pop-up.
- Mises à jour.

Les ressources du GIP Cyber malveillance : les mises à jour.

FAUX SUPPORT

EN DIRECT

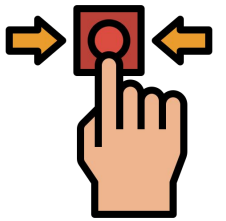
QUE FAIRE :



> Ne pas paniquer (un ordinateur se répare).

> Les procédures à suivre

- Ne pas appeler le numéro suggérer sur l'écran, le sms, le mail...
- Déblocage de l'écran (touches, gestionnaire, arrêt).
- Ne pas donner d'informations sensibles (carte, mot de passe).
- Ne rien installer, ne pas donner la main sur son appareil.



> Trouver de l'aide

FAUX SUPPORT

LES AIDES

COMMENT ACCOMPAGNER UN BÉNÉFICIAIRE PIRATÉ ?

> Donner une check-list

- Récupérer le maximum d'informations
- Opposition bancaire
- Technique (retrait des applications, analyses)
- Prévenir l'entourage et les structures d'aides
- Porter plainte

> Travailler avec les accompagnés sur des exercices de prévention.

> Les rassurer sur leurs capacités, leurs connaissances et leurs compétences.

FAUX SITE

LES AIDES

LES ÉLÉMENTS DE BASE À COMMUNIQUER

> Donner une check-list des éléments à vérifier :

- Lecture d'une page et des informations d'un site (cadenas, mentions légales…)
- Toujours faire le parallèle avec la vie courante (offres alléchantes)
- Où trouver des avis clients, comment faire une recherche (plateformes de vérifications, forums de consommateur, applications)

Les ressources du GIP Cyber malveillance : guider les achats en ligne

FAUX SITES

LES SOLUTIONS

COMMENT LES AIDER :

> Procédures à suivre :

- Institutions et services (dépôt de plainte).
- Les aides pour les accompagner (associations, gouvernementales).
- Signaler les sites pour les bloquer.

La liste des contacts de l'institut national de la consommation.

Le centre de contact Info Escroqueries de l'Etat.

L'outil de signalement de la CNIL.

La démarche en ligne de signalement des sites de phishing

PENSE BÊTE

GRANNY GEEK VOUS CONSEILLE

> Accompagner, prévenir et renseigner.

> Utiliser des exemples de la vie courante pour leur rappeler que c'est aussi du bon sens.

> Prévoir des chapitres sur la sécurité à chaque accompagnement.

> Aucun support officiel ne contactera directement par mail, sms ou appel téléphonique pour demander de modifier des mots de passe ou demander de l'argent.

> Trouver une phrase de rappel simple : « Si vous avez un doute, il n'y a pas de doute ».

NOUS VOUS REMERCIONS POUR VOTRE PARTICIPATION