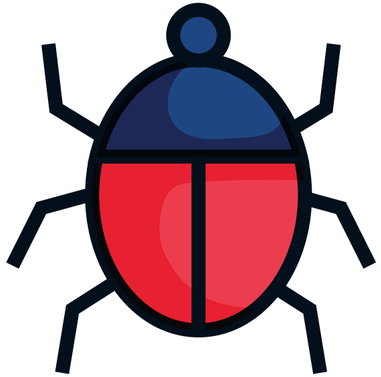
SENSIBILISATION A LA CYBERSECURITE

à destination des seniors

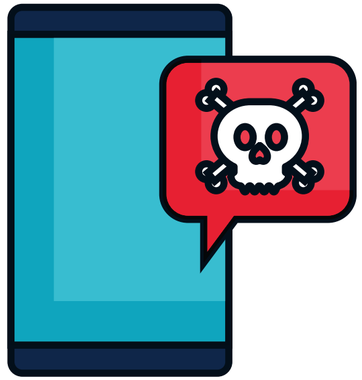
OBJECTIFS D'APPRENTISSAGE

A l'issue de cette formation, vous serez en mesure de maîtriser :

Les dangers d'internet



Les principales attaques cyber



Le harcèlement en ligne

Les bonnes pratiques cyber

Pour anticiper/détecter les menaces et savoir réagir.

1. LES DANGERS D'INTERNET

DES USAGES AUX MENACES

Vous utilisez Internet pour répondre à plusieurs de vos besoins de relations sociales, de communication et information :

- Communiquer (mail et réseaux sociaux)
- S'informer sur l'actualité ou d'autres thèmes qui vous concernent
- Se renseigner sur des produits
- Faire des achats

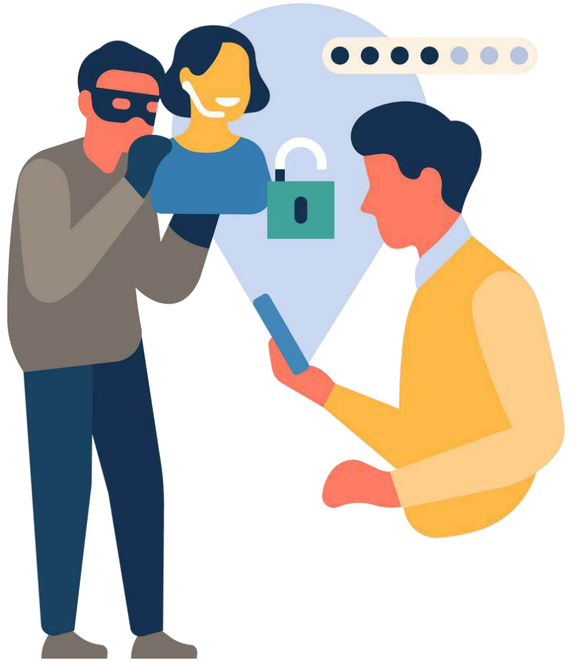
Mais quels sont les risques?

- Vol d'accès
- Vol d'argent
- Vol de données

CIBLER L’UTILISATEUR

Pour les escrocs les internautes seniors apparaissent souvent comme une cible plus facile à tromper :

- services de rencontres,
- demandes d’aide ou de dons,
- promesses de traitements et remèdes miracles,
- ventes aux enchères en ligne ou sites de vente non officiels,
- fausses informations ou injonctions à payer.



Tous ces procédés sont d’autant **plus efficace** s’ils ont été orientés grâce à **l’étude de votre profil et des données sur vous** (publiques ou volées).


CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

CIBLER LE SYSTEME INFORMATIQUE

Un virus est un programme malveillant dont le but est de survivre sur un système informatique et d'en parasiter les ressources (données, mémoire, réseau).

- installé après ouverture d'un document compromis (téléchargé ou PJ),
- téléchargé et installé après un clic sur un lien,
- perturbe le fonctionnement du système,
- donne accès à distance au système,
- exporte des données…

Pour sa propagation, **un virus utilise tous les moyens disponibles :** messagerie, partage de fichiers, portes dérobées, page internet frauduleuse, clés USB…

CONSO MAG

LES VIRUS INFORMATIQUES : COMMENT S'EN PROTÉGER ?

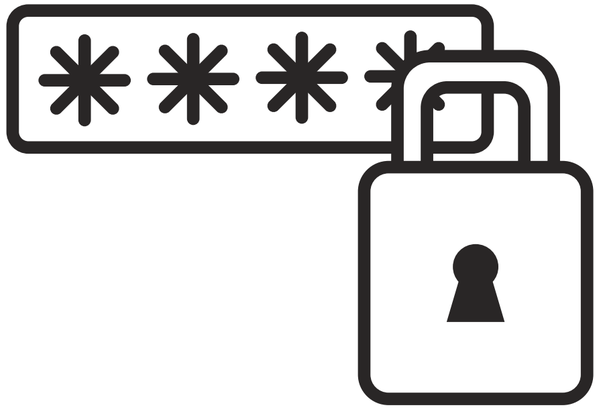
TEMPS D'ECHANGE

Quels sont les dangers d’internet que vous avez retenu ?

D’après vous, comment peut-on les éviter ?

2. LES CYBERATTAQUES

Les menaces d'internet



VOL DE MOTS DE PASSE

VOL DE DONNEES PERSONNELLES

VOL D'ARGENT

Qu'est ce qu'une cyberattaque?

Utilisation d'internet par des personnes malveillantes pour dérégler à distance les ordinateurs

Son but ?

Voler des informations pour les effacer ou les échanger contre de l'argent

Comment est-elle réalisée ?

Test de plusieurs mots de passe
Envoi de milliers de mails infestés par des virus
Création de faux sites internet malades

TEMPS D'ECHANGE

Quels sont les dangers que vous avez rencontré ?

Comment ça s'est passé ?

ATTAQUES DES MOTS DE PASSE

La tentation est forte d'avoir une gestion trop simple des mots de passe. Une telle pratique est dangereuse, car elle augmenterait considérablement les risques de compromettre la sécurité de vos accès.

Un virus est un programme malveillant dont le but est de survivre sur un système informatique et d'en parasiter les ressources (données, mémoire, réseau).

- les attaquants essayent de deviner les mots de passe,
- en effectuant des tests aléatoires,
- en utilisant un dictionnaire,
- en exécutant un logiciel qui teste toutes les possibilités.
  en 2022 il faut 1 heure pour « casser » un MdP à 9 caractères (Majuscules, minuscules, chiffres)
- en utilisant des listes de mots de passe vendues par des pirates

N'utilisez pas vos mots de passe sur un ordinateur partagé et changez votre mot de passe au moindre soupçon.

Pourquoi dit-on mot de passe et pas mot de passoire ?

Les attaques sur les mots de passes

Essayer de deviner tous les mots de passe, en effectuant des tests aléatoires, en utilisant un dictionnaire ou un logiciel.

Les conséquences?

- Vol d'informations
- Vol d'argent
- Vol de noms/ prénoms

Le phishing

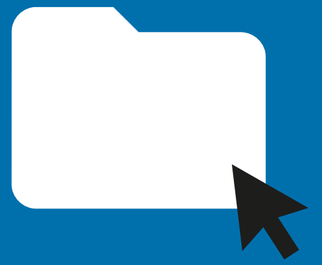
L'hameçonnage est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles

- Les identifiants et mots de passes,
- Les accès bancaires,
- Les numéros des moyens de paiement,
- En se faisant passer pour un tiers de confiance.

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.

Comment pêcher un numéro de carte bancaire ?

Les rançongiciels/ransomwares



C’est un logiciel malveillant qui bloque l’accès à l’ordinateur ou à des données en les chiffrant et qui réclame à la victime le paiement d’une rançon.

- Après l’ouverture d’une pièce jointe,
- Après avoir cliqué sur un lien malveillant reçu dans des courriels,
- En naviguant sur des sites compromis,
- Suite à une intrusion sur le système

Il est de plus en plus courant que les données chiffrées soient en plus exfiltrées, pour être revendues ou servir de moyen de chantage supplémentaire.

TEMPS D'ECHANGE

Comment vous protegez-vous ?

Appliquez-vous déjà certains conseils parmi eux ? Si oui, lesquels ?

Comment s'en protéger ?

- Ne jamais partager ses informations personnelles (noms, prénoms, adresses maison/école...)
- Ne pas croire tout ce qu'il y'a sur internet
- Créer des mots de passe en utilisant des phrases de passe
- Demander aux parents d'installer et mettre à jour régulièrement ses antivirus
- En cas d'insultes, prévenir un adulte ou un parent

SI VOUS ÊTES VICTIME DE RANSOMWARE, IL NE FAUT SURTOUT PAS PAYER DE RANCON.

SE RENDRE DANS UN COMMISSARIAT DE POLICE OU A LA GENDARMERIE POUR DEPOSER UNE PLAINTE.

3. L'HARCELEMENT EN LIGNE

TEMPS D'ECHANGE

D’après vous, qu’est-ce que l’harcèlement en ligne ?

Avez-vous déjà victime/témoin d’un acte de cyberharcèlement ?

Comment avez-vous réagi ?

LE CYBERHARCELEMENT

QU'EST CE QUE LE CYBERHARCELEMENT ?

Lorsqu'une personne reçoit, sur Internet ou sur son téléphone portable des messages contenant des insultes, des menaces, des vidéos embarrassantes, des moqueries et des humiliations répétées.

QUELLES SONT LES CONSEQUENCES ?

Tristesse, solitude. perte de confiance en soi, dépression, pensées suicidaires.

IL EST NECESSAIRE D'ETRE BIEN AVERTI SUR LE CYBERHARCELEMENT

SI VOUS ETES TEMOIN OU VICTIME

N'HESITEZ PAS A VOUS RAPPROCHER DES AUTORITES OU APPELER LE 3018

4. LES BONNES PRATIQUES CYBER

Mots de passe

Voici 10 bonnes pratiques à adopter pour gérer efficacement vos mots de passe

01 utilisez un mot de passe différent pour chaque service

02 utilisez un mot de passe suffisamment long et complexe

03 utilisez un mot de passe impossible à deviner

04 utilisez un gestionnaire de mots de passe

05 changez votre mot de passe au moindre soupçon

06	ne communiquez jamais votre MdP à un tiers
07	n’utilisez pas vos mots de passe sur un ordinateur partagé
08	activez la « double authentification* » lorsque c’est possible
09	changez les mots de passe par défaut des différents service
10	choisissez un mot de passe particulièrement robuste pour votre messagerie

LA MINUTE INFO

CONNECTÉ ET PROTÉGÉ

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Renforcer la sécurité

Voici 10 bonnes pratiques à adopter pour la sécurité de vos appareils.

01 appliquez les bonnes pratiques sur les mots de passes

02 soyez vigilant sur internet et lorsque vous recevez des mails

03 installez et mettez à jour un antivirus

04 analysez l'ordinateur regulierement

05 appliquez les mises à jour de sécurité

06 n’installez des applications que depuis les sites officiels

07 faites des sauvegardes et conservez les en sécurité

08 ne connectez pas de supports de mémoire (usb, hdd,…) inconnus

09 scannez le support externe par l’antivirus avant usage

10 évitez les réseaux wifi publics ou inconnus

Pour sa propagation, un virus utilise tous les moyens disponibles : messagerie, partage de fichiers, portes dérobées, page internet frauduleuse, clés USB…

LE PHISING

Mesures préventives.
ne communiquez jamais d’informations sensibles par messagerie ou téléphone ,
avant de cliquer sur un lien douteux, placez le curseur de votre souris sur ce lien,
vérifiez l’adresse du site qui s’affiche dans votre navigateur,
en cas de doute, contactez si possible directement l’organisme concerné.

!

Si vous êtes victime.
si vous avez communiqué des éléments sur vos moyens de paiement
FAITES OPPOSITION IMMÉDIATEMENT

si vous avez communiqué un mot de passe
CHANGEZ-LE IMMÉDIATEMENT

CONSO MAG

QUE FAIRE POUR NE PAS ETRE VICTIME D'HAMEÇONNAGE ?

LES RANCONGICIELS / RANSOMWARE

Mesures préventives.
appliquez les mises à jour de sécurité des applications et de l'antivirus,
soyez vigilant avec les messages, d'expéditeurs inconnus,
n'installez pas d'application ou de programme « piratés »,
évitez les sites non sûrs ou illicites (HTTPS),
faites des sauvegardes régulières,
gestion des MdP et des droits Admin,
éteindre un ordinateur non utilisé.

Si vous êtes victime.

!

débranchez la machine d'internet
ne payez pas la rançon
conservez les preuves
portez plainte et faites-vous assister par des professionnels qualifiés.

LA MINUTE INFO

CONNECTÉ ET PROTÉGÉ

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

DISPOSITIF NATIONAL D'ASSISTANCE

AUX VICTIMES D'ACTES DE CYBERMALVEILLANCE

www.cybermalveillance.gouv.fr

QUIZ POUR UN CYBERCHAMPION !

QUESTION 1 : QUE FAIRE LORSQU'ON REÇOIT UN MESSAGE D'UN ÉTRANGER QUI NOUS DEMANDE DE TÉLÉCHARGER UN FICHIER ?

01 TRANSFÉRER LE MESSAGE À UNE AUTRE PERSONNE

02 TÉLÉCHARGER ET OUVRIR LE FICHIER

03 VÉRIFIER L'IDENTITÉ DE L'EMETTEUR EN VÉRIFIANT LES COORDONNÉES DE CONTACT

04 AUCUNE RÉPONSE N'EST VRAIE

QUESTION 1 : QUE FAIRE LORSQU'ON REÇOIT UN MESSAGE D'UN ÉTRANGER QUI NOUS DEMANDE DE TÉLÉCHARGER UN FICHIER ?

01 TRANSFÉRER LE MESSAGE À UNE AUTRE PERSONNE

02 TÉLÉCHARGER ET OUVRIR LE FICHIER

03 VÉRIFIER L'IDENTITÉ DE L'EMETTEUR EN VÉRIFIANT LES COORDONNÉES DE CONTACT

04 AUCUNE RÉPONSE N'EST VRAIE

QUESTION 2 : COMMENT RÉAGIR LORSQU'ON EST VICTIME D'UNE CYBER ATTAQUE ?

01 DÉCONNECTER L'ORDINATEUR D'INTERNET

02 FAIRE UN SCAN DE L'APPAREIL AVEC L'ANTIVIRUS POUR VÉRIFIER S'IL EST INFECTÉ

03 MODIFIER TOUS LES MOTS DE PASSE ET DÉPOSER UNE PLAINTE À LA GENDARMERIE

04 TOUTES LES REPONSES SONT VRAIES

QUESTION 2 : COMMENT RÉAGIR LORSQU'ON EST VICTIME D'UNE CYBER ATTAQUE ?

01 DÉCONNECTER L'ORDINATEUR D'INTERNET

02 FAIRE UN SCAN DE L'APPAREIL AVEC L'ANTIVIRUS POUR VÉRIFIER S'IL EST INFECTÉ

03 MODIFIER TOUS LES MOTS DE PASSE ET DÉPOSER UNE PLAINTE À LA GENDARMERIE

04 TOUTES LES REPONSES SONT VRAIES

QUESTION 3 : LES VIRUS INFORMATIQUES SONT UN TYPE DE CYBERATTAQUE ?

01 VRAI

02 FAUX

QUESTION 3 : LES VIRUS INFORMATIQUES SONT UN TYPE DE CYBERATTAQUE ?

01 VRAI

02 FAUX

QUESTION 4 : QUELS SONT LES INDICES DE PHISHING PARMI LES PROPOSITIONS SUIVANTES ?

01 LES ERREURS D'ORTHOGRAPHES/GRAMMAIRE DANS LE MESSAGE

02 LES ADRESSES ÉLECTRONIQUES INCORRECTES OU FAUSSES

03 DES PHRASES QUI INCITENT À UNE RÉPONSE URGENTE

04 TOUTES LES RÉPONSES SONT VRAIES

QUESTION 4 : QUELS SONT LES INDICES DE PHISHING PARMI LES PROPOSITIONS SUIVANTES ?

01 LES ERREURS D'ORTHOGRAPHES/GRAMMAIRE DANS LE MESSAGE

02 LES ADRESSES ÉLECTRONIQUES INCORRECTES OU FAUSSES

03 DES PHRASES QUI INCITENT À UNE RÉPONSE URGENTE

04 TOUTES LES RÉPONSES SONT VRAIES

QUESTION 5 : LORSQUE JE SUIS ENTRAIN D'UTILISER UN APPAREIL MOBILE ET QUE J'AI BESOIN DE ME DÉPLACER, QUE FAIRE ?

01 JE ME DÉPÊCHE D'ALLER FAIRE CE QUE J'AI À FAIRE

02 JE ME M'ASSURE DE METTRE EN VEILLE MON APPAREIL OU DE L'ÉTEINDRE

03 JE ME DÉPLACE AVEC MON APPAREIL

04 AUCUNE DES RÉPONSES N'EST VRAIE

QUESTION 5 : LORSQUE JE SUIS ENTRAIN D'UTILISER UN APPAREIL MOBILE ET QUE J'AI BESOIN DE ME DÉPLACER, QUE FAIRE ?

01 JE ME DÉPÊCHE D'ALLER FAIRE CE QUE J'AI À FAIRE

02 JE ME M'ASSURE DE METTRE EN VEILLE MON APPAREIL OU DE L'ÉTEINDRE

03 JE ME DÉPLACE AVEC MON APPAREIL

04 AUCUNE DES RÉPONSES N'EST VRAIE

QUESTION 6 : QUELLES SONT LES PRATIQUES À ADOPTER POUR ÉVITER DE SUBIR UNE CYBERATTAQUE ?

01 UTILISER DES MOTS DE PASSE SÛRS ET FAIRE DES COPIES DE SES FICHIERS

02 EFFECTUER DES MISES À JOUR DES APPAREILS ET INSTALLER DES ANTI-VIRUS À JOUR

03 NE PAS CONNECTER SUR DES WIFI PUBLICS ET NE PAS OUVRIR DES MAILS DOUTEUX

04 TOUTES LES RÉPONSES SONT VRAIES

QUESTION 6 : QUELLES SONT LES PRATIQUES À ADOPTER POUR ÉVITER DE SUBIR UNE CYBERATTAQUE ?

01 UTILISER DES MOTS DE PASSE SÛRS ET FAIRE DES COPIES DE SES FICHIERS

02 EFFECTUER DES MISES À JOUR DES APPAREILS ET INSTALLER DES ANTI-VIRUS À JOUR

03 NE PAS CONNECTER SUR DES WIFI PUBLICS ET NE PAS OUVRIR DES MAILS DOUTEUX

04 TOUTES LES RÉPONSES SONT VRAIES

QUESTION 7 : QUELLE EST LA MENACE COMMUNE À TOUTES LES CYBERATTAQUES ?

01 VOL D'INFORMATIONS ET ARNAQUES

02 TRAHISON

03 TROMPERIE

04 CYBERHARCELEMENT

QUESTION 7 : QUELLE EST LA MENACE COMMUNE À TOUTES LES CYBERATTAQUES ?

01 VOL D'INFORMATIONS ET ARNAQUES

02 TRAHISON

03 TROMPERIE

04 CYBERHARCELEMENT

QUESTION 8 :QUEL EST LE MEILLEUR TYPE DE MOT DE PASSE

01 CELUI QUI CONTIENT MA DATE DE NAISSANCE

02 CELUI QUI LE NOM DE MON ANIMAL DE COMPAGNIE OU CELUN DE L'UN DE MES PROCHES

03 CELUI QUI EST LE PLUS COURT POSSIBLE

04 CELUI QUI CONTIENT MINIMUM 08 CARACTÈRES DIFFÉRENTS OU UNE PHRASE DE PASSE

QUESTION 8 :QUEL EST LE MEILLEUR TYPE DE MOT DE PASSE

01 CELUI QUI CONTIENT MA DATE DE NAISSANCE

02 CELUI QUI LE NOM DE MON ANIMAL DE COMPAGNIE OU CELUN DE L'UN DE MES PROCHES

03 CELUI QUI EST LE PLUS COURT POSSIBLE

04 CELUI QUI CONTIENT MINIMUM 08 CARACTÈRES DIFFÉRENTS OU UNE PHRASE DE PASSE

QUESTION 9 : QUEL EST L'INTRUS ?

01 Ransomware

02 Cyberharcelement

03 Attaque sur les mots de passe

04 Phishing

QUESTION 9 : QUEL EST L'INTRUS ?

01 Ransomware

02 Cyberharcelement

03 Attaque sur les mots de passe

04 Phishing

QUESTION 10 : JE PEUX ME CONNECTER SUR LES RESEAUX WIFI PUBLICS (HÔPITAUX,GARES,TRAINS,RESTAURANTS) SANS AUCUN PROBLÈME

01 Faux

02 Vrai

QUESTION 10 : JE PEUX ME CONNECTER SUR LES RESEAUX WIFI PUBLICS (HÔPITAUX,GARES,TRAINS,RESTAURANTS) SANS AUCUN PROBLÈME

01 Faux

02 Vrai

QUESTION 11 : INSTALLER UN ANTIVIRUS SUR MES APPAREILS MOBILES EST SUFFISANT POUR ME PROTÉGER CONTRE LES CYBERATTAQUES

01 Faux

02 Vrai

QUESTION 11 : INSTALLER UN ANTIVIRUS SUR MES APPAREILS MOBILES EST SUFFISANT POUR ME PROTÉGER CONTRE LES CYBERATTAQUES

01 Faux

02 Vrai

IL EST NECESSAIRE D’ETRE BIEN AVERTI SUR LES MENACES DE CYBERSECURITE ET DE SAVOIR S’EN PROTEGER

MAIS LE PLUS IMPORTANT EST DE :

FAIRE PREUVE DE BON SENS