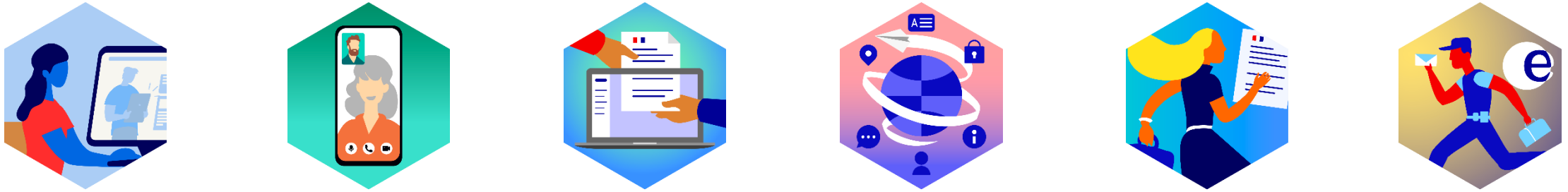


Opération soutenue par l'État dans le cadre du dispositif
Conseiller numérique France Services

**www.conseiller-numerique.gouv.fr**

Département des Landes

CONSEILLER NUMÉRIQUE France services

Financé par GOUVERNEMENT Liberté Égalité Fraternité

FRANCE RELANCE

Financé par l'Union européenne NextGenerationEU

# Cybersécurité: sécurisez vos usages numériques

## Parcours intermédiaire : atelier 12

CC BY NC SA

*Julien Daudigeos - 2022*

# Avant de commencer…

- Pour vous, quelles sont les menaces sur le WEB ?
- Comment pensez-vous vous en protéger ?

# Objectif de l'atelier

- Découvrir les bonnes pratiques pour sécuriser vos usages numériques.

# Quelles sont les menaces ?

Logiciels malveillants (malware)

Virus

Rançongiciel (ransomware)

Usurpation d'identité

Vol de données


Hameçonnage (phishing)

Arnaque au faux support technique

Arnaque sur les réseaux sociaux

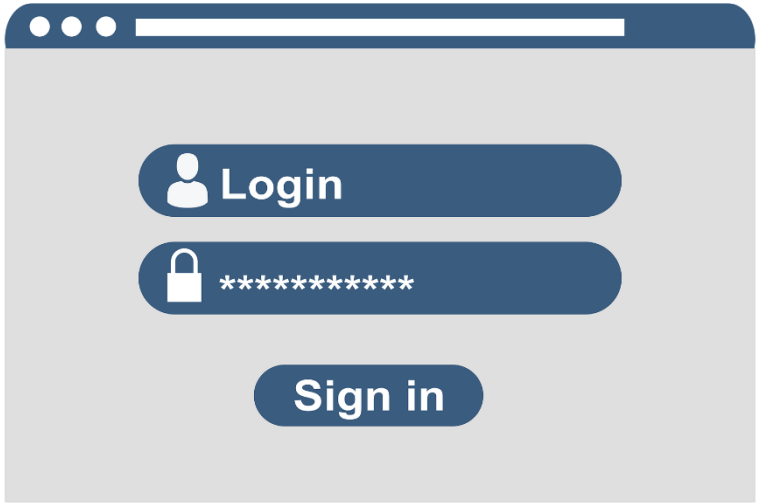
Faux sites
Faux profils

# Pour mieux protéger

# vos usages numériques…

# Mots de passe sécurisés

Pour chaque site Web qui nécessite un compte, il faut un mot de passe !




Nous allons voir quelques bonnes pratiques pour les rendre les plus forts possible !

# Mots de passe sécurisés

- ✓ Longueur : 8 caractères minimum, 12 caractères c'est mieux !
- ✓ Avoir au moins une majuscule, une minuscule, un chiffre et un caractère spécial.
- ✓ Ne pas utiliser d'info personnelles (nom, prénom, date de naissance…)
- ✓ Faire en sorte qu'il soit impossible à deviner
- ✓ Ne jamais communiquer vos mots de passe
- ✓ Un mot de passe différent pour chaque service
- ✓ Utiliser un gestionnaire de mot de passe

# Mots de passe sécurisés

| TEMPS NÉCÉSSAIRE POUR TROUVER UN MOT DE PASSE AVEC LA MÉTHODE DE L'ATTAQUE PAR FORCE BRUTE EN 2022 | | | | | |
|---|---|---|---|---|---|
| Nombre de caractères | Nombres uniquement | Minuscules | Minuscules et majuscules | Nombres, Majuscules et Minuscules | Nombres, Majuscules, Minuscules et caractères spéciaux |
| 4 | Instantanément | Instantanément | Instantanément | Instantanément | Instantanément |
| 5 | Instantanément | Instantanément | Instantanément | Instantanément | Instantanément |
| 6 | Instantanément | Instantanément | Instantanément | Instantanément | Instantanément |
| 7 | Instantanément | Instantanément | 2 secondes | 7 secondes | 31 secondes |
| 8 | Instantanément | Instantanément | 2 minutes | 7 minutes | 39 minutes |
| 9 | Instantanément | 10 secondes | 1 heure | 7 heures | 2 ans |
| 10 | Instantanément | 4 minutes | 3 jours | 3 semaines | 5 mois |
| 11 | Instantanément | 2 heures | 5 mois | 3 ans | 34 ans |
| 12 | 2 secondes | 2 jours | 24 ans | 200 ans | 3000 ans |
| 13 | 19 secondes | 2 mois | 1000 ans | 12 000 ans | 202 000 ans |
| 14 | 3 minutes | 4 ans | 64 000 ans | 750 000 ans | 16 millions d'an. |
| 15 | 32 minutes | 100 ans | 3 millions d'années | 46 millions d'an. | 1 milliard d'an. |
| 16 | 5 heures | 3000 ans | 173 millions d'an. | 3 milliards d'an. | 92 milliards d'an. |
| 17 | 2 jours | 69 000 ans | 9 milliards d'an. | 179 milliards d'an. | 7 billions d'an. |
| 18 | 3 semaines | 2 millions d'années | 467 milliards d'an. | 11 billions d'an. | 438 billions d'an. |
| SOURCE : HIVE SYSTEMS > hivesystems.io/password | | | | | |

# Testons des mots de passe !

# Antivirus et pare feu

Un **antivirus** est un programme informatique qui sert à **identifier**, **neutraliser**, et **éliminer** les virus informatiques.

Certains sont gratuits et d'autres payants.

Il est **impératif** d'avoir un antivirus !

**Windows Defender** (installé sur les ordinateurs Windows) est performant.

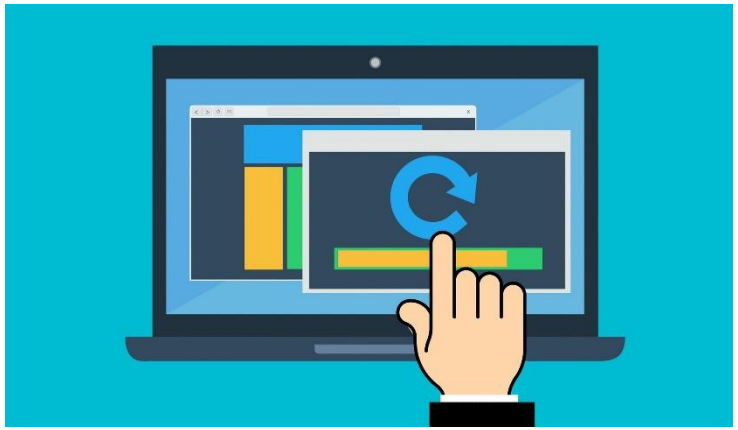
Le **pare feu** est un logiciel qui régule les communications d'un réseau.

# Mise à jour de votre ordinateur et de vos logiciels

✓ **Les mises à jour importantes ou critiques** corrigent des failles de sécurité qui peuvent être utilisées pour pirater votre équipement.

✓ Certaines mises à jour se font **automatiquement** sur les appareils.

✓ Faites les mises à jour qui vous sont proposées **dés que possible** !



# Être vigilant avec les mails reçus (ou SMS)

- ✓ **L'hameçonnage (phishing en anglais)** est une technique de piratage qui vise à vous piéger pour vous dérober des informations confidentielles (mots de passe, informations d'identité ou bancaires).

- ✓ Le pirate envoie un virus contenu dans une pièce-jointe qu'on vous incite à ouvrir, ou un lien qui vous attirerait sur un site malveillant.

- ✓ En cas de réception d'un message inattendu ou alarmiste par mail ou SMS, il ne faut **ni répondre ni cliquer sur les liens ou pièce-jointes**.

# Le phishing en vidéo

Comment reconnaitre une tentative de phishing

# Repérer une tentative de phishing

- ✓ Un email d'un service ou d'une société **dont vous n'êtes pas client**
- ✓ Un nom **d'expéditeur inhabituel**, une adresse mail **fantaisiste, bizarre**
- ✓ Un message (ou son objet) **trop alléchant ou alarmiste**
- ✓ Une **apparence suspecte**
- ✓ Une demande **d'informations confidentielles**
- ✓ Une **incitation à cliquer** sur un lien ou une pièce-jointe

# Repérer une tentative de phishing


Bonjour ,

Nous vous informons que vous avez un remboursement en attente d'un montant de **169,20 €** sur votre espace personnel.

La carte enregistrée sur votre espace personnel n'a pas été créditée pour le motif suivant :

Le numéro de mobile enregistré sur votre espace personnel ne correspond pas à celui associé à votre compte bancaire.

**Détails de remboursement:**

---

Référence : AWL-20/982KDJ
Montant: : **169,20 €**

---

Pour accepter le paiement rapide en ligne, cliquez sur le lien suivant et sélectionnez une méthode de remboursement.

- Modifier mes informations personnelles.

Votre assurance maladie
18 5375 Boulevard de Vaugirard, 75015 Paris, France

# Repérer une tentative de phishing

ING

Chère cliente, Cher client,

Lors de votre dernier opération bancaire, nous avons remarqué une activité inhabituelle sur votre compte.

Pour réactiver votre compte Vous devez mettre à jour vos informations, une fois ces dernières validées, le compte fonctionnera normalement.

L'ensemble du processus ne prendra que 5 minutes. Vous devez agir maintenant pour résoudre le problème le plus rapidement possible.

Suivez le lien ci-dessous pour finaliser le processus et régler l'état de votre compte

Accèder à votre espace sécurisé

Nous vous remercions de votre confiance

Cordialement,

Arnaud Le Roux
Direction Qualité

# Repérer une tentative de phishing

**De :** service client
**Date :** jeudi 21 octobre 2021 à 03:33
**À :** [redacted]
**Cc :**
**Objet :** SOCGEN@FRANCE.FR

SOCIETE GENERALE

Bonjour,

**Un conseiller vous a adressé un nouveau message important.**

NOUS VOUS INVITONS À LE(S) CONSULTER

En cliquant sur le lien ci - dessous :

Accéder Au Message

PENSEZ À PROTÉGER NOTRE PLANÈTE,
N'imprimez cet e-mail et vos documents que si nécessaire.

Société Générale

*La rubrique "Mes relevés en ligne" n'est pas encore accessible depuis votre Appli mobile Société Générale

# Repérer une tentative de phishing

Message du 20/10/21 02:10
De : "Group Service" <pimkles@dfyoxc.owler.com>
A :
Copie à :
Objet : Asurance Maladie | Ameli.Fr

# Téléchargements

- ✓ N’installez des applications et logiciels que depuis les **sites ou magasins officiels**.

- ✓ De même, évitez les sites Internet suspects ou frauduleux (téléchargement, vidéo, streaming illégaux) qui pourraient également installer un virus sur vos matériels.

# Sauvegarde

- ✓ En cas de perte, de vol, de panne, de piratage ou de destruction de vos appareils numériques, vous perdrez les données enregistrées sur ces supports.

- ✓ Il peut s'agir de **données importantes** à vos yeux (photos, vidéos, documents personnels ou de travail, etc.).

- ✓ Ayez le réflexe de réaliser **régulièrement** une sauvegarde de vos données.

- ✓ Les sauvegardes peuvent se faire **sur disque dur** externe, sur **clé USB** ou sur un **espace de stockage en ligne (cloud).**

# Coordonnées bancaires

✓ Soyez particulièrement vigilants avec coordonnées bancaires !

✓ Évitez de les enregistrer sur votre navigateur.

✓ Aucun service de l'État, aucune banque, aucune assurance ne vous demandera vos coordonnées bancaires par mail ou SMS !

# Être vigilant sur les réseaux sociaux

✓ Vos comptes de réseaux sociaux peuvent contenir des **informations personnelles sensibles** qui intéressent les cybercriminels !

✓ Pour que personne ne puisse usurper votre identité, protégez bien l'accès à votre compte avec un mot de passe unique et robuste !

✓ Attention également aux **faux profils** et **faux comptes**, ne faites confiance qu'aux personnes que vous connaissez réellement.

✓ Vérifiez vos **paramètres de confidentialité**

# Pour aller plus loin

Le site cybermalveillance.gouv.fr

# Avez-vous des questions ???

# Merci pour votre attention !