

À LA DÉCOUVERTE DE LA SÉCURITÉ INFORMATIQUE

Page 1 – Comprendre les risques

1/5
pages

INFORMER
SENSIBILISER
ACCOMPAGNER
PROGRESSER
EN TOUTE
SÉRÉNITÉ !

UN
AVENIR
PLUS SÛR
POUR TOUS !

ENSEMBLE
POUR UN
NUMÉRIQUE
PLUS SÛR !

APPRENDRE
COMPRENDRE
AGIR
ENSEMBLE !

La sécurité
informatique,
c'est l'affaire
de tous !

Petits gestes,
grands effets !

1 Pourquoi se protéger ?

La sécurité informatique protège tes données personnelles, tes appareils et ton travail.

Elle évite les pertes, les vols et les problèmes qui peuvent avoir des conséquences importantes dans ta vie quotidienne et professionnelle.



Mes données

Photos, documents, comptes, informations personnelles



Mes appareils

Ordinateur, téléphone, tablette...



Mon travail

Fichiers, projets, mails, etc.

Se protéger, c'est garder le contrôle sur sa vie numérique !

2 Virus et malware

Les virus et les logiciels malveillants (malware) sont des programmes conçus pour nuire à ton ordinateur ou à tes données.

Ils peuvent se cacher dans un fichier, un lien ou une pièce jointe, et s'installer sans que tu le saches.

Oh non !
Même un simple
fichier peut être
dangereux !



Ils peuvent :

- endommager tes fichiers
- ralentir ton ordinateur
- voler tes données
- afficher des publicités indésirables

Un antivirus et des mises à jour régulières aident à te protéger !

3 Phishing (hameçonnage)

Le phishing consiste à envoyer de faux e-mails ou messages qui semblent provenir d'une organisation de confiance (banque, administration, entreprise...).

Le but est de te faire cliquer sur un lien, de télécharger un fichier ou de te faire communiquer des informations sensibles (mot de passe, numéro de carte, etc.).



De : support@banque-secu.com
Objet : Action requise !

Bonjour,
Votre compte sera suspendu si vous ne confirmez pas vos données. [Cliquez ici](#) pour éviter la fermeture.

Je me connecte

FAUX !

Ce message
semble vrai !
Il faut vraiment
être vigilant...

Vérifie toujours l'expéditeur, le contenu et ne clique pas sur un lien douteux !

4 Mots de passe faibles

Un mot de passe trop simple ou utilisé partout est un vrai risque. S'il est découvert, un attaquant peut accéder à tous tes comptes (e-mail, réseaux sociaux, banque...).

Plus ton mot de passe est unique et complexe, plus tes comptes sont en sécurité !

À éviter :

- 123456
- azerty
- motdepasse
- votreprenom
- date de naissance

Trop simples
et facilement
devinables !

À privilégier :

- B7@Soleil!2024
- Au moins 12 caractères
- Des lettres, des chiffres
- Des caractères spéciaux
- Différent pour chaque compte

Un mot de passe robuste
et unique !

5 Récapitulons !

Voici l'essentiel
à retenir !

- La sécurité informatique protège tes données, tes appareils et ton travail.
- Les virus et malware peuvent endommager tes fichiers et ralentir ton ordinateur.
- Le phishing utilise de faux messages pour te piéger.
- Un mot de passe faible peut donner accès à tous tes comptes.
- Adopte des gestes simples et vigilants au quotidien.



À RETENIR :

La cybersécurité commence par des gestes simples et quotidiens !

Des compétences d'aujourd'hui pour demain !

Apprendre • Comprendre • Agir
Ensemble !

Eric Schaefer — Formateur bureautique, numérique et informatique



DES PERSONNES
PLUS AUTONOMES



DES USAGES
PLUS SÛRS



UN NUMÉRIQUE
PLUS RESPONSABLE

INFORMER
SENSIBILISER
ACCOMPAGNER
PROGRESSER
EN TOUTE
SÉRÉNITÉ !

À LA DÉCOUVERTE DE LA SÉCURITÉ INFORMATIQUE

Page 2 – Mots de passe et double authentification

2/5

APPRENDRE
AUJOURD'HUI
AGIR DEMAIN

Des conseils
simples et concrets,
pour moi aussi !

SÉCURITÉ
BONNES PRATIQUES
VIE NUMÉRIQUE SÉRÈNE

1 Créer un mot de passe solide

Un bon mot de passe
doit être :

- ✓ **Long**
Au moins 12 caractères
(idéalement plus).
- ✓ **Unique**
Un mot de passe différent
pour chaque compte.
- ✓ **Difficile à deviner**
Un mélange de lettres,
chiffres et caractères
spéciaux.



Tr3fle!Bleu7Nuage@25



Plus c'est long et varié, plus c'est difficile à pirater !

2 Phrase de passe

Une phrase de passe
est plus facile
à retenir et tout aussi
voire plus sûre !

On peut utiliser une phrase
qui a du sens pour vous,
en y ajoutant des chiffres
et un symbole.

Une phrase est plus longue,
plus naturelle à retenir
et plus résistante aux attaques !



MonChatAimeLesVacances2024!

3 À éviter

Évitez ces mots de passe
trop simples et ne les réutilisez
jamais sur plusieurs sites !

- ✗ 123456
- ✗ azerty
- ✗ motdepasse
- ✗ Votre nom ou votre date de naissance
- ✗ password
- ✗ P@ssw0rd



TROP
FACILE !

NE PAS
RÉUTILISER
LE MÊME MOT DE PASSE
SUR PLUSIEURS COMPTES !

4 Double authentification (2FA)

La double authentification
ajoute une deuxième étape
en plus de votre mot de passe.

Même si quelqu'un
trouve mon mot de passe,
il ne pourra pas se connecter
sans le deuxième code !



5 Récapitulons !

Avec ces bonnes pratiques,
je surfe plus sereinement !

- ✓ J'utilise un mot de passe long, unique et difficile à deviner.
- ✓ Je peux utiliser une phrase de passe.
- ✓ Je n'utilise pas de mots de passe simples.
- ✓ Je ne réutilise jamais le même mot de passe.
- ✓ J'active la double authentification (2FA) quand c'est possible.

À RETENIR :
Un bon mot de passe
+ la 2FA renforcent
fortement votre sécurité.

Petits gestes,
grande protection !



Eric Schaefer — Formateur bureautique, numérique et informatique



DES PERSONNES
PLUS AUTONOMES



DES USAGES
PLUS SÛRS



UN NUMÉRIQUE
PLUS RESPONSABLE

Apprendre • Comprendre • Agir
Ensemble !



INFORMER
SENSIBILISER
ACCOMPAGNER
PROGRESSER
EN TOUTE
SÉRÉNITÉ !

À LA DÉCOUVERTE DE LA SÉCURITÉ INFORMATIQUE

Page 3 – Repérer le phishing et les pièces jointes suspectes

3/5
pages

DES
COMPÉTENCES
D'AUJOURD'HUI
POUR DEMAIN !

1 Un e-mail douteux ? Plusieurs signes doivent vous alerter !

De : service-client@securite-info.com

Objet : **URGENT** : Votre compte sera bloqué !

Bonjour,
Votre compte sera suspendu dans 24h.
Cliquez **immédiatement** sur le lien ci-dessous
pour le réactiver :

Activer mon compte

Cordialement,
L'équipe Sécurité

Un expéditeur
suspect ou inhabituel !

Un ton urgent
qui fait peur !

Des fautes
d'orthographe !

Un lien à cliquer
(à éviter !)

Des fautes
d'orthographe !

Les pirates du web
jouent sur l'urgence
et la peur pour vous
faire agir trop vite !

Un e-mail officiel
ne vous met jamais
la pression !

2 Vérifier l'expéditeur et le lien Avant de cliquer, prenez le temps de vérifier !

De : support@securite-info.com

À : moi@monentreprise.fr

Objet : Mise à jour de votre compte

Vérifiez bien l'adresse
de l'expéditeur :
une adresse étrange
(peu familière, avec des
fautes ou un autre nom
de domaine) est suspecte.

Ça ressemble
presque au vrai...
mais ce n'est pas
la bonne adresse !

Surveillez le lien avec votre souris (sans cliquer) :

Cliquez ici pour mettre à jour votre compte

https://securite-info.com_mauvais-site.net/compte

Surveillez, vérifiez,
et si un doute persiste :
ne cliquez pas !

Le lien affiché n'est pas
le même que le texte :
c'est un site frauduleux !

Un petit geste
de vérification
peut vous éviter
de gros ennuis !

3 Pièces jointes Méfiez-vous des fichiers inattendus !

Un e-mail avec une pièce jointe non attendue
peut contenir un virus ou un programme malveillant.

De : facture@service-pro.com
Objet : Facture de septembre

Facture_septembre.exe
(2,3 Mo)

Je ne m'attendais
pas à recevoir
cette pièce jointe...
Mieux vaut
ne pas l'ouvrir !

Les types de fichiers les plus à risque :

- .exe (programmes)
- .scr (économiseurs d'écran)
- .bat (scripts)
- .js (scripts JavaScript)
- .zip (fichiers compressés)
- .docm, .xlsm (documents avec macros)

Un fichier peut
paraître inoffensif
mais contenir
un danger caché !

4 Que faire ? Les bons réflexes à adopter !



Ne pas cliquer
sur le lien.



Ne pas répondre
au message.



Signaler le message
à votre service
informatique.



Supprimer le message
s'il vous semble
suspect.

En cas de doute,
mieux vaut prévenir
que guérir !

5 Récapitulons ! Les points essentiels à retenir !

- ✓ Je me méfie des e-mails inattendus ou urgents.
- ✓ Je vérifie l'expéditeur et le lien avant de cliquer.
- ✓ Je n'ouvre pas de pièce jointe inconnue.
- ✓ Je signale tout message suspect à mon service informatique.
- ✓ Je supprime les messages douteux.

À RETENIR !

En cas de doute,
on vérifie avant
de cliquer !

Des compétences d'aujourd'hui
pour demain !



DES PERSONNES
PLUS AUTONOMES



DES USAGES
PLUS SÛRS



UN NUMÉRIQUE
PLUS RESPONSABLE

Apprendre • Comprendre • Agir
Ensemble !

Eric Schaefer — Formateur bureautique, numérique et informatique

À LA DÉCOUVERTE DE LA SÉCURITÉ INFORMATIQUE

4/5

Page 4 - Mises à jour, sauvegardes et Wi-Fi

INFORMER
SENSIBILISER
ACCOMPAGNER
PROGRESSER
EN TOUTE
SÉRÉNITÉ !



Mettre à jour,
sauvegarder, utiliser
un Wi-Fi sécurisé :
des gestes simples
qui font une grande
différence !

Un appareil à jour,
des données bien
gardées, un Wi-Fi
en toute sécurité !

C'est clair !
Avec ces bons réflexes,
je protège mes données
et je navigue plus
sereinement !

UN
NUMÉRIQUE
PLUS SÛR
POUR UN
AVENIR
MEILLEUR !



LA
SÉCURITÉ
C'EST L'AFFAIRE
DE TOUS !



SÉCURITÉ

BONNES PRATIQUES

VIE NUMÉRIQUE SÉRÈNE

APPRENDRE
PARTAGER
PROGRESSER
ENSEMBLE !



1 POURQUOI METTRE À JOUR ?

- ✓ Les mises à jour corrigent des failles de sécurité.
- ✓ Elles améliorent le fonctionnement.
- ✓ Elles protègent contre de nouvelles menaces.



Un appareil non mis à jour
est une porte d'entrée
pour les pirates !

2 MISES À JOUR AUTOMATIQUES



- ✓ Activez les mises à jour automatiques sur vos appareils (ordinateur, smartphone, tablette...).
- ✓ Les correctifs s'installent sans intervention.
- ✓ Vous êtes protégé en continu, sans y penser !

Simple à activer, grande tranquillité !

3 SAUVEGARDER SES DONNÉES



- ✓ Faites des sauvegardes régulières de vos fichiers importants (photos, documents...).
- ✓ Sur un disque dur externe (localement).
- ✓ Ou dans le cloud (espace en ligne sécurisé).
- ✓ En cas de panne, de vol, de ransomware ou d'erreur, vos données restent accessibles !

Vos souvenirs et vos documents méritent d'être protégés !

4 Wi-Fi ET RÉSEAUX PUBLICS



Réseau sécurisé
(WPA2/WPA3)

- ✓ Privilégiez les réseaux Wi-Fi sécurisés (mot de passe, WPA2/WPA3).
- ✓ Évitez les réseaux publics (hôtels, aéroports, cafés...), pour vos actions sensibles (banque, achats, données perso).
- ✓ Si besoin, utilisez un VPN pour chiffrer votre connexion.
- ✓ Vérifiez toujours le nom du réseau pour éviter les faux points d'accès.

Sur un Wi-Fi public,
restez prudent : ne partagez pas
d'informations sensibles !

5 RÉCAPITULONS !



- ✓ Je mets mes appareils à jour.
- ✓ J'active les mises à jour automatiques.
- ✓ Je sauvegarde régulièrement mes données (sur un disque externe ou dans le cloud).
- ✓ J'utilise des réseaux Wi-Fi sécurisés.
- ✓ J'évite les actions sensibles sur un Wi-Fi public.

À RETENIR

Un appareil à jour
et des sauvegardes
régulières limitent
les risques.

Des petits gestes
de grands effets !



Des compétences d'aujourd'hui
pour demain !

Apprendre • Comprendre • Agir
Ensemble !

Eric Schaefer – Formateur bureautique, numérique et informatique



DES PERSONNES
PLUS AUTONOMES



DES USAGES
PLUS SÛRS



UN NUMÉRIQUE
PLUS RESPONSABLE

INFORMER
SENSIBILISER
ACCOMPAGNER
PROGRESSER
EN TOUTE
SÉRÉNITÉ !



À LA DÉCOUVERTE DE LA SÉCURITÉ INFORMATIQUE

Page 5 – Données personnelles, RGPD et bonnes pratiques

5/5

UN
NUMÉRIQUE
PLUS SÛR
POUR UN
AVENIR
MEILLEUR !



Mes données
m'appartiennent !
Je les protège
et je choisis
à qui je les partage !

Des gestes simples
pour plus de sécurité
au quotidien !

Nos données
personnelles ont de la
valeur. Apprenons à les
protéger ensemble !

DES COMPÉTENCES
D'AUJOURD'HUI
POUR DEMAIN !

Ensemble
pour un
numérique
plus sûr !



1 Données personnelles

Ce sont toutes les informations
qui permettent de vous identifier.



Nom
Prénom



Adresse
e-mail



Numéro
de téléphone



Photo



Données
bancaires

Ces informations vous concernent,
elles sont précieuses !

2 Partager avec prudence

Ne partagez que ce qui est
vraiment nécessaire et vérifiez
toujours à qui vous vous
adressez.



Avant de partager,
posez-vous la question :
« Est-ce vraiment
nécessaire ? »

Et est-ce
la bonne
personne ?



Un message peut vite faire le tour...
Réfléchissez avant de cliquer !

3 RGPD

Le RGPD (Règlement Général
sur la Protection des Données) est une loi
européenne qui protège vos données
personnelles et encadre leur utilisation.



- ✓ Vous avez des droits
- ✓ Vos données sont protégées
- ✓ Leur utilisation est encadrée
- ✓ Vous gardez le contrôle

Le RGPD renforce votre vie privée
et votre confiance dans le numérique !

4 Les bons réflexes au quotidien

Des gestes simples pour mieux protéger vos données
au bureau comme à la maison.



Verrouiller
sa session

Protégez votre
accès quand vous
vous absentez.



Mettre à jour
ses appareils

Les mises à jour
corrigent des failles
de sécurité.



Être vigilant
en cliquant

Méfiez-vous des liens
et pièces jointes
suspects.



Garder un espace
de travail rangé

Ne laissez pas
de documents
sensibles visibles.



Stocker
sécurisé

Utilisez des solutions
fiables (espace sécurisé,
cloud de confiance...).

5 Récapitulons !

- ✓ Je connais mes données personnelles et leur valeur.
- ✓ Je partage avec prudence.
- ✓ Je comprends que le RGPD me protège.
- ✓ J'adopte les bons réflexes au quotidien.
- ✓ Je reste vigilant et responsable.

Des citoyens numériques
plus responsables, pour un monde plus sûr !

À RETENIR

Protéger
les données,
c'est protéger
les personnes.



Eric Schaefer — Formateur bureautique, numérique et informatique

Des compétences d'aujourd'hui
pour demain !

Apprendre • Comprendre • Agir
Ensemble !



DES PERSONNES
PLUS AUTONOMES



DES USAGES
PLUS SÛRS



UN NUMÉRIQUE
PLUS RESPONSABLE