

LE NUMÉRIQUE
EST UN OCÉAN
PLEIN DE PIÈGES
MAIS ENSEMBLE
ON APPREND
À NAVIGUER
EN SÉCURITÉ !



À L'ABORDAGE DES CYBERATTQUES

5
pages

Une BD pédagogique pour comprendre les menaces,
éviter les pièges et adopter les bons réflexes

S'INFORMER
COMPRENDRE
ANTICIPER
ÉVITER
AGIR !



Matelots,
les cyberattaques
sont partout !

Mais pas de panique !
avec les bons réflexes,
nous restons
maîtres à bord !

PHISHING



SMISHING

SMS

VISHING



QUISHING



MALWARE



RANSOMWARE



Regarde capitaine !
Ils arrivent de tous
les côtés !

Chaque navire
cache un piège
numérique !

Alors on se forme
et on se protège !

Ensemble,
on est plus
forts !

MIEUX
CONNAÎTRE
LES RISQUES
POUR MIEUX
SE PROTÉGER



DES
CONNAISSANCES
AUJOURD'HUI,
PLUS DE LIBERTÉ
DEMAIN !



AU PROGRAMME DE CES 5 PAGES

1



Comprendre les cyberattaques

Qu'est-ce que c'est ?
Pourquoi elles
se multiplient ?
Qui sont les pirates
numériques ?

2



Les pièges des messages

Phishing, smishing,
vishing, quishing...
Apprendre à les repérer
et à s'en méfier !

3



Malwares et ransomwares

Des logiciels malveillants
qui infectent vos appareils
et peuvent bloquer
vos données.
Comment les éviter ?

4



Mots de passe et faux sites

Des mots de passe solides,
les dangers des faux sites
et comment reconnaître
les arnaques ?

5



Wi-Fi public, deepfake et bons réflexes

Les risques des réseaux
Wi-Fi, les faux contenus
(deepfake) et tous les
bons réflexes pour
naviguer sereinement !



Eric Schaefer — Formateur bureautique, numérique et informatique



DES PERSONNES
PLUS AUTONOMES



DES USAGES
PLUS SÛRS



UN NUMÉRIQUE
PLUS RESPONSABLE



Apprendre
Comprendre • Agir
Ensemble !

DES MESSAGES BIEN FAITS PEUVENT SEMBLER TRÈS RÉELS, MAIS CE SONT PARFOIS DES PIÈGES!



LES PIÈGES DES MESSAGES

Phishing, smishing, vishing et quishing

Page 2/5

MÊMES MENACES, MÊMES RÉFLEXES, PLUS ENSEMBLE, PLUS FORTS!



Des QR codes piégés!

QUISHING



PAR QR CODE

Des appels manipulés!

VISHING



PAR TÉLÉPHONE

Des SMS trompeurs!

SMISHING

SMS

PAR SMS

Des e-mails qui piègent!

PHISHING



PAR E-MAIL

Là-bas !
Quatre navires ennemis utilisent nos moyens de communication pour nous piéger ! Apprenons à les reconnaître !

Ils utilisent des e-mails, des SMS, des appels et même des QR codes ?!

Oui ! Les pirates du numérique jouent sur la confiance et l'urgence !

Mais avec les bons réflexes, on les déjoue !

On reste vigilants et on protège l'équipage !

UN MESSAGE SUSPECT ? ON VÉRIFIE ! ON RÉFLÉCHIT ! ON DEMANDE CONSEIL !

LA SÉCURITÉ EST L'AFFAIRE DE TOUS ! MIEUX INFORMÉS = MIEUX PROTÉGÉS!



1 PHISHING

Des e-mails frauduleux pour voler vos données



Des e-mails qui imitent des organisations connues pour vous inciter à cliquer et à donner vos informations (identifiants, mots de passe, données bancaires...).

2 SMISHING

Des SMS frauduleux



Des SMS qui vous incitent à cliquer sur un lien pour voler vos données ou installer un logiciel malveillant sur votre téléphone.

3 VISHING

Des appels frauduleux



Des appels de faux conseillers qui se font passer pour votre banque, un service connu... pour vous soutirer vos codes ou informations sensibles.

4 QUISHING

Des QR codes piégés



Des QR codes qui redirigent vers des sites frauduleux pour voler vos données ou installer un malware sur votre appareil.

MES 4 BONS RÉFLEXES

1 **Vérifier l'expéditeur**

Je regarde bien l'adresse e-mail, le numéro ou l'expéditeur du message.

2 **Ne pas cliquer dans l'urgence**

Je prends le temps de réfléchir, même si le message semble urgent ou attractif.

3 **Ne jamais donner ses codes par téléphone**

Une vraie banque ne demande jamais vos mots de passe ou codes par téléphone !

4 **Scanner seulement des QR codes de confiance**

Je vérifie la source du QR code et préfère ceux provenant de personnes ou d'organisations fiables.

Eric Schaefer — Formateur bureautique, numérique et informatique



DES PERSONNES PLUS AUTONOMES



DES USAGES PLUS SÛRS



UN NUMÉRIQUE PLUS RESPONSABLE



Apprendre Comprendre • Agir Ensemble!

DES PROGRAMMES
MALVEILLANTS
PEUVENT SE CACHER
PARTOUT :
DANS UN E-MAIL,
UN FICHIER,
UNE CLÉ USB...
RESTONS VIGILANTS !

MALWARES ET RANSOMWARES

Page
3/5

Les pièges cachés à bord

CONNAÎTRE
CES MENACES,
C'EST DÉJÀ
SE PROTÉGER !

Ces programmes
malveillants ont l'air
inoffensifs, mais ils sont
des pirates numériques !
Apprenons à les repérer
pour éviter qu'ils ne
prennent le contrôle
de notre navire !

1 MALWARE DÉGUISE

Un programme qui a l'air utile
mais qui cache une menace.



Il peut s'installer sans
qu'on le remarque et ouvrir
la porte aux cybercriminels !

2 SPYWARE / KEYLOGGER

Des logiciels qui espionnent
votre activité et enregistrent
vos frappes clavier.



Ils peuvent
voir les sites
que vous visitez,
vos messages
et même vos
mots de passe !

3 PIÈCES JOINTES PIÉGÉES

Des fichiers reçus par e-mail
qui contiennent des virus
ou des macros malveillantes.



Même un e-mail
qui semble officiel
peut contenir
un piège !

Fiche de paie
Avril.docm

4 CLÉ USB INCONNUE

Une clé USB trouvée ou reçue
peut contenir des logiciels
malveillants qui s'installent
automatiquement.



Ne branchez jamais
une clé USB d'origine
inconnue, même
si elle semble
inoffensive !

5 RANSOMWARE

Un logiciel qui chiffre vos fichiers
et bloque l'accès à vos données
en demandant une rançon.



Vos photos, documents
et fichiers peuvent être bloqués
tant que vous ne payez pas !

Avec les bons
réflexes, on garde
le contrôle du
navire !

Waouh !
Ils peuvent se
cacher n'importe
où !

Il faut vraiment
faire attention
à ce qu'on ouvre
et à ce qu'on
branche !

Mieux vaut
prévenir que
payer une rançon !

LES
CYBERATTQUES
NE PRENNENT
PAS DE VACANCES !



LES BONS RÉFLEXES À TOUJOURS GARDER EN TÊTE !



1 Télécharger
depuis des sources
officielles

Uniquement des sites
et logiciels de confiance.



2 Mettre à jour
ses appareils

Les mises à jour
corrigent des failles
de sécurité.



3 Utiliser un
antivirus fiable

Il détecte et bloque
de nombreux
programmes
malveillants.



4 Se méfier
des pièces jointes

Ne pas ouvrir un fichier
ou un lien suspect,
même s'il semble
officiel !



5 Ne jamais brancher
une clé USB
inconnue

Elle peut contenir
des virus qui s'installent
automatiquement.



6 Sauvegarder
régulièrement
ses fichiers

Sur un support externe
ou dans le cloud
pour les récupérer
en cas d'attaque.



Eric Schaefer — Formateur bureautique, numérique et informatique



DES PERSONNES
PLUS AUTONOMES



DES USAGES
PLUS SÛRS



UN NUMÉRIQUE
PLUS RESPONSABLE



Apprendre
Comprendre
Agir
Ensemble !

DES
COMPTES BIEN
PROTÉGÉS,
C'EST UNE
ÉQUIPE PLUS
SÛRE EN MER
NUMÉRIQUE !

MOTS DE PASSE ET FAUX SITES

Page
4/5

Éviter les pièges d'identité

Équipage !
Les pirates ne forcent plus
toujours la porte... ils se
font passer pour vous !
Voyons ensemble comment
protéger vos comptes !

Ah oui !
Un mot de passe
faible, c'est comme
une porte sans
serrure !

Et si on reçoit
plein de demandes
de connexion,
on accepte ?

S'INFORMER
COMPRENDRE
ANTICIPER
ÉVITER
AGIR !

Mieux vaut
être méfiant !
On vérifie
toujours !

1 MOT DE PASSE TROP FAIBLE

Un mot de passe court et simple
est facile à deviner pour les pirates !

Mot de passe :

123456

⚠ Trop faible !
En quelques secondes,
il est trouvé !

Les pirates
utilisent des
outils qui testent
des millions
de mots de passe
très courants !

123456
password
azerty
qwerty
soleil2024
...

123456 ?
Trop facile !

2 RÉUTILISATION DES MOTS DE PASSE

Utiliser le même mot de passe
sur plusieurs sites est très risqué !
Si un site est piraté, tous vos comptes
peuvent être compromis !



Mot de passe : Marine2024 ⚠



Mot de passe : Marine2024 ⚠



Mot de passe : Marine2024 ⚠



Mot de passe : Marine2024 ⚠

Un seul mot de passe compromis
peut donner accès à tous vos comptes !

3 CREDENTIAL STUFFING

Les pirates utilisent des identifiants
volés sur un site pour se connecter
automatiquement sur d'autres sites.

N	Netflix	✓ Connecté !
a	Amazon	✗ Échec
S	Spotify	✗ Échec
G	Google	✓ Connecté !
B	Banque	✗ Échec

Je teste des milliers
de combinaisons
de comptes piratés...
Ça marche parfois !

Même si vous n'avez rien fait de mal,
vos comptes peuvent être piratés
à cause d'une fuite sur un autre site !

4 PAGES DE CONNEXION FACTICES (FAUX SITES)

Les pirates créent de fausses pages qui ressemblent
en tous points à de vrais sites pour voler vos identifiants.

✓ Vrai site

https://www.google.com

Google

julien@mail.fr

.....

Se connecter

⚠ Faux site

http://google-secure.com

Google

julien@mail.fr

.....

Se connecter

Vérifiez toujours
l'adresse du site
et la présence du
HTTPS !
Même une petite
différence peut
cacher un faux site !

Regardez bien
l'adresse !
Il suffit parfois
d'une lettre en plus
pour se faire piéger !

5 MFA FATIGUE (DEMANDES RÉPÉTÉES DE VALIDATION)

Les pirates envoient de multiples demandes
de validation (double authentification) en espérant
que vous finissiez par accepter par erreur.



Si vous n'êtes pas
en train de vous connecter,
et que vous recevez
des demandes répétées,
N'ACCÉPTEZ PAS !
C'est une attaque !

On dirait
que quelqu'un
a mon mot de passe !
Je refuse
tout ce que je n'ai pas
demandé !

RÉCAP' : LES BONS RÉFLEXES !

- ✓ Utiliser des mots de passe longs et uniques pour chaque compte
- ✓ Ne jamais réutiliser un mot de passe
- ✓ Vérifier l'adresse du site et le HTTPS
- ✓ Activer la double authentification (2FA)
- ✓ Refuser toute demande de connexion non sollicitée

DES PETITS
GESTES POUR
DE GRANDS
EFFETS !



Rester vigilants
ensemble !
La meilleure défense,
c'est vous !

DES
COMPTES
SÉCURISÉS
POUR DE NOUVELLES
AVENTURES !



Eric Schaefer — Formateur bureautique, numérique et informatique



DES PERSONNES
PLUS AUTONOMES



DES USAGES
PLUS SÛRS



UN NUMÉRIQUE
PLUS RESPONSABLE



Apprendre
Comprendre • Agir
Ensemble !

MÊMES
MENACES
NOUVEAUX
PIÈGES
RESTONS
VIGILANTS !



WI-FI PUBLIC, DEEPFAKE ET BONS RÉFLEXES

Naviguer prudemment jusqu'au port

Page

5/5

UN
INTERNET
PLUS SÛR,
C'EST UN
ÉQUIPAGE
PLUS FORT !



1

WI-FI PUBLIC : UN ACCÈS À RISQUES

Un Wi-Fi public
peut être piégé !
Des pirates peuvent
intercepter vos données
(mots de passe, e-mails,
données bancaires...).

On croit être
en sécurité...
mais ils nous
observent !



ÉVITEZ LES WI-FI PUBLICS
OU UTILISEZ UN VPN !

2

PUBLICITÉS TROMPEUSES ET FAUX TÉLÉCHARGEMENTS

Waouh !
Photoshop gratuit ?
-90 % ? C'est tentant !

Stop !
Ces publicités peuvent
cacher des virus.
Vous téléchargez
peut-être un malware
au lieu du vrai logiciel !

SI C'EST
TROP BEAU
POUR ÊTRE VRAI,
C'EST SÛREMENT
UN PIÈGE !



3

FAUX SUPPORT TECHNIQUE

Des pirates se font passer
pour un support technique
(Microsoft, Apple, votre banque...)
pour vous faire installer un logiciel,
prendre le contrôle de votre appareil
ou vous faire payer !

Oh ! Il faut
appeler ?
Ça a l'air
officiel...

⚠ Votre ordinateur
est infecté !
Appelez maintenant :
01 23 45 67 89
Assistance immédiate

AUCUNE ENTREPRISE
SÉRIEUSE NE VOUS
DEMANDERA UN ACCÈS
À DISTANCE
PAR TÉLÉPHONE !



4

FAUX PROFILS ET DEEPFAKE SUR LES RÉSEAUX SOCIAUX

Regardez !
Mon acteur préféré
m'envoie un message
personnel ! Incroyable !

Ces messages, photos ou
vidéos peuvent être créés
par intelligence artificielle.
On peut aujourd'hui
imiter la voix et l'apparence
de quelqu'un de très
réaliste !

Salut !
C'est moi !
J'ai un cadeau
rien que pour toi !
Clique ici ! ❤️

FAUX !

VÉRIFIEZ
TOUJOURS
PAR UN AUTRE
CANAL !



5

QUE FAIRE EN CAS DE DOUTE ?

Un message bizarre ?
Un appel inattendu ?
Je ne sais pas si c'est vrai...

Prenez le temps de réfléchir,
vérifiez l'information
et demandez de l'aide.
Mieux vaut perdre une minute
que se faire piéger !

PORT SÛR
en ligne aussi !

CAP SUR
UN INTERNET
PLUS SÛR !

UN BON
RÉFLEXE AUJOURD'HUI,
UN ÉQUIPAGE
EN SÉCURITÉ
DEMAIN !



À RETENIR



Éviter les Wi-Fi publics
ou utiliser un VPN

Protégez vos données
sur des réseaux de confiance.



Se méfier des appels
et messages non sollicités

Ne donnez jamais vos informations
et n'installez pas de logiciel
à la demande d'un inconnu.



Vérifier par un autre canal

En cas de doute, contactez
la personne ou l'entreprise
depuis un site officiel
ou un autre moyen.



Demander de l'aide
en cas de doute

Parlez-en à un collègue,
un proche ou au service
informatique.



Ne pas se précipiter

Prenez le temps de réfléchir.
Un instant de prudence
peut vous éviter bien
des problèmes.

LES BONS
RÉFLEXES
NOUS MÈNENT
TOUJOURS
AU BON PORT !



Eric Schaefer — Formateur bureautique, numérique et informatique



DES PERSONNES
PLUS AUTONOMES



DES USAGES
PLUS SÛRS



UN NUMÉRIQUE
PLUS RESPONSABLE



Apprendre
Comprendre • Agir
Ensemble !



MIEUX COMPRENDRE LES RISSQUES POUR NAVIGUER EN SÉCURITÉ !