magnétic

# FORMATION
# INITIATION À LA CYBERSÉCURITÉ

# votre formateur

## Thomas Joiris

### Développeur back-end chez Magnétic

8 ANS D'EXPÉRIENCE

CERTIFICATION OPQUAST

Développeur PHP · Symfony
NodeJS · Base de données
Architecture logicielle · SaaS

t.joiris@magnetic.coop

# Objectifs

## Pourquoi cet atelier sur la cybersécurité ?

- Obligation ?
- Les cibles des cyberattaques ?
- Principale porte d'entrée des attaques ?
- Coût moyen d'une cyberattaque ?
- Temps pour craquer un mot de passe de 8 caractères ?

# Objectifs

## Pourquoi cet atelier sur la cybersécurité ?

- Obligation **légale** (RGPD article 32)
- Environ 60% des attaques ciblent les TPE et PME
- L'**erreur humaine** est la plus exploitée : **email** 73%
- Coût moyen d'une cyber-attaque : 59 000€
- Password de 8 caractères craqués en 37 secondes
- Bref, de b**onnes habitudes** pro et perso

### Sources

- https://www.cybermalveillance.gouv.fr
- https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article32
- https://www.cci-paris-idf.fr/sites/default/files/2021-01/etude-cybersecurite-09-28_-_version_cci_france.pdf

# Exemples

## Quelques cas récents…

- Le Louvre (mot de passe, systèmes obsolètes)
- Piratage de Free de 2024
- Ransomware d’un proche

# Les types

## Les attaques

- Ransomware (rançongiciel)
- DDoS
- XSS
- Brute-force

## Les fraudes

- Phishing (hameçonnage)
- Mail spoofing
- Fuite de données

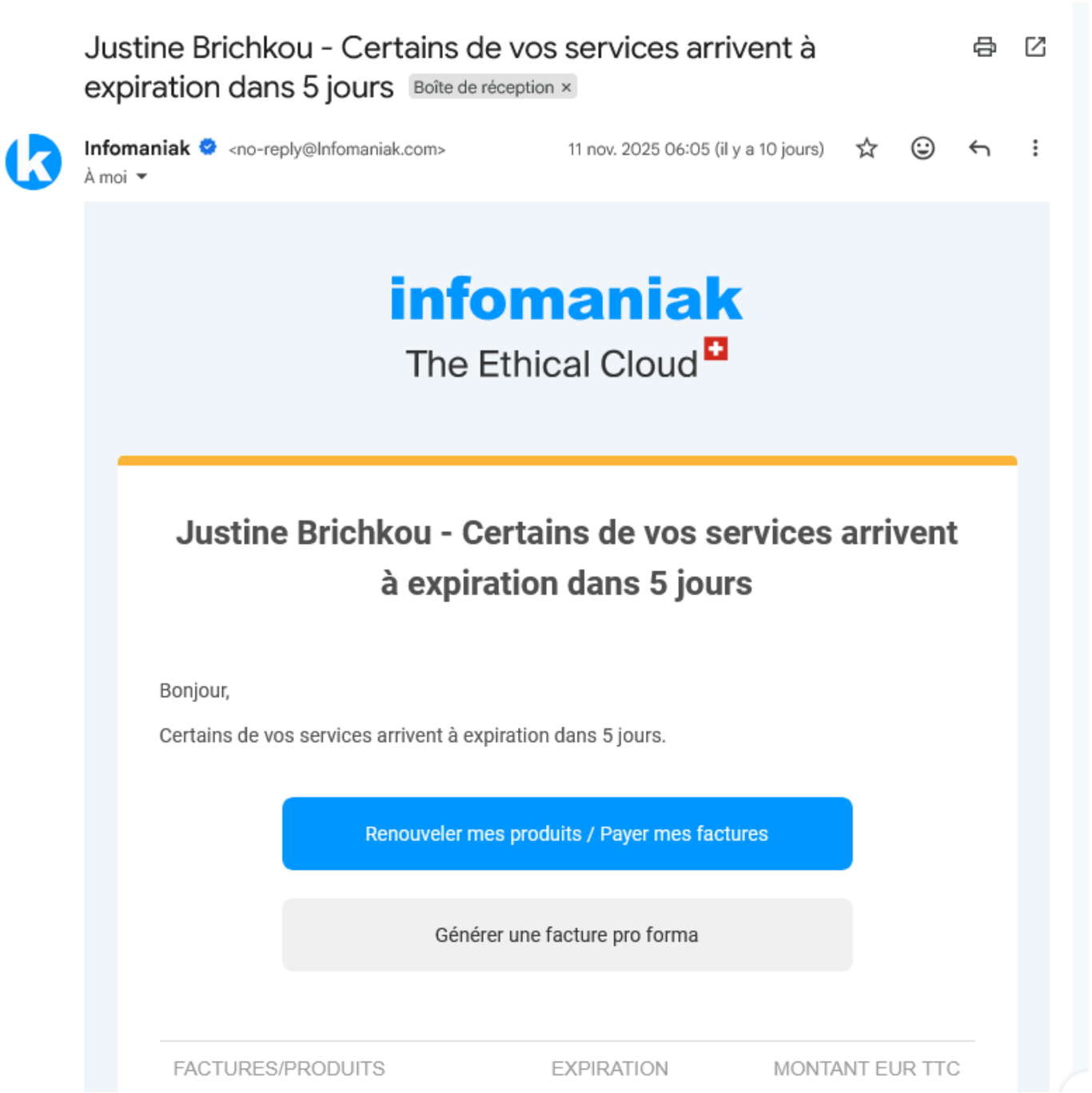
# ÉTUDES DE CAS

# Ransomware

Une agence lyonnaise reçoit une facture qui semble venir d'une fournisseur habituel...

Justine, la comptable, clique sur la pièce-jointe et...

# Ransomware



Justine Brichkou - Certains de vos services arrivent à expiration dans 5 jours Boîte de réception ×

**Infomaniak** <no-reply@Infomaniak.com> 11 nov. 2025 06:05 (il y a 10 jours)

À moi

infomaniak

The Ethical Cloud

**Justine Brichkou - Certains de vos services arrivent à expiration dans 5 jours**

Bonjour,

Certains de vos services arrivent à expiration dans 5 jours.

Renouveler mes produits / Payer mes factures

Générer une facture pro forma

FACTURES/PRODUITS EXPIRATION MONTANT EUR TTC

# Ransomware

Un petit logiciel s'est lancé : un **ransomware** (rançongiciel).
En deux heures : tout les fichiers de l'agence étaient chiffrés.

Et sur tout les ordinateurs : un message de rançon.

```
Votre réseau a été pénétré.

Tous les fichiers de chaque machine de votre réseau ont été chiffrés avec un puissant algorithme.

Vos backups ont été chiffrés ou supprimés.

Nous sommes les seuls à posséder le logiciel permettant de décrypter vos systèmes.

Vous pouvez  nous contacter à l'adresse [redacted]

N'ÉTEIGNEZ PAS VOTRE ORDINATEUR - les fichiers pourraient être endommagés.
NE RENOMMEZ PAS ET NE DÉPLACEZ PAS les fichiers chiffrés et les README.
NE SUPPRIMEZ PAS les README.
Cela pourrait amener à l'impossibilité de récupérer certains de vos fichiers.

BTC wallet:
1BvBMSE[redacted]W2

Aucun système n'est protégé.
```

# Ransomware

## Conséquences

- Trois semaines d'arrêt.
- Ils ont dû renvoyer 4 clients majeurs qui attendaient des livrables. **Perte** de 80 000€ de chiffre d'affaires.
- **Racheter** tous les **logiciels** (15 000€).
- Payer un expert en cybersécurité (8 000€).
- Reconstituer manuellement ce qui pouvait l'être.
- Racheter du matériel compromis (5 000€).

**Coût total estimé** : 28 000€ hors impact sur le CA, 108 000€ total

Plus grave encore : leur **réputation**. Deux ans après, ils ont encore du mal à retrouver le niveau d'activité d'avant l'attaque.

# Ransomware

## Et vous ? Qu'auriez-vous fait ?

# Ransomware

## Comment éviter ce genre de situation ?

1. **Vérifier** l'adresse email (un "i" est différent de "l")
2. L'urgence **inhabituelle** dans le corps du message
3. Les **fautes** dans le message
4. Le type de **pièce-jointe** (.zip vs .pdf, et jamais les .exe)

# Ransomware

## Les adresses e-mail

L'identifiant local

**t.joiris+123@magnetic.coop**

Le domaine

L'extension

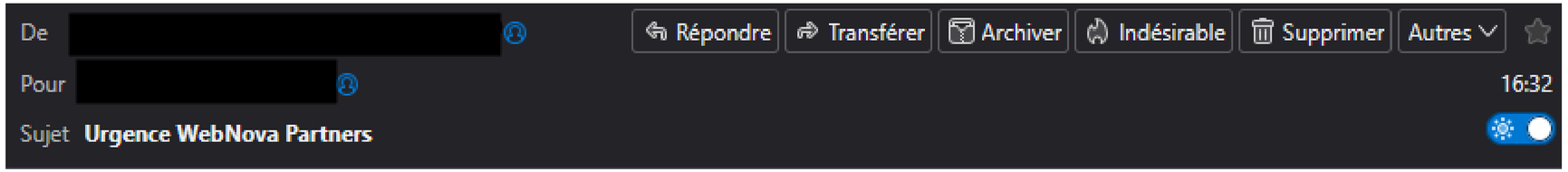
Le caractère séparateur

# Phishing

Sam est un graphiste freelance de Nantes, il travaille avec une dizaine de clients réguliers.

Un mercredi après-midi, il reçoit un e-mail urgent...

# Phishing




Bonjour,

Je vous contacte en urgence.
Plusieurs visiteurs nous ont signalé qu'ils obtenaient actuellement une **erreur 500** en accédant au site. C'est une situation extrêmement problématique pour nous : nous avons une campagne en cours et chaque minute compte.

Comme vous travaillez avec nous depuis longtemps, je sais que vous avez déjà dû intervenir en urgence par le passé. Là encore, j'aurais besoin que vous **me transfériez immédiatement les accès FTP** afin que je puisse corriger le bug avant que la direction ne remonte ce problème.

Merci de passer par notre portail sécurisé pour transmettre les identifiants : https://support-technique-verif.webnova-partners.pro/urgence-ftp

**David Morelo**
Support Technique – *WebNova Partners*

# Phishing

## Conséquences

La page se charge, puis affiche une erreur.
Sauf que c'était un vrai formulaire.

Dans les 30 minutes, les hackers se connectent au serveur avec les identifiants volés. Ils ont modifié le site du client.

- Le client s'aperçoit du problème le lendemain matin quand un visiteur le contacte.
- Le site est blacklisté par Google
- 200 ordinateurs de visiteurs ont été infectés.
- Le client porte plainte contre le graphiste
- 15 000€ de dommage et intérêts

# Phishing

## Et vous ? Qu'auriez-vous fait ?

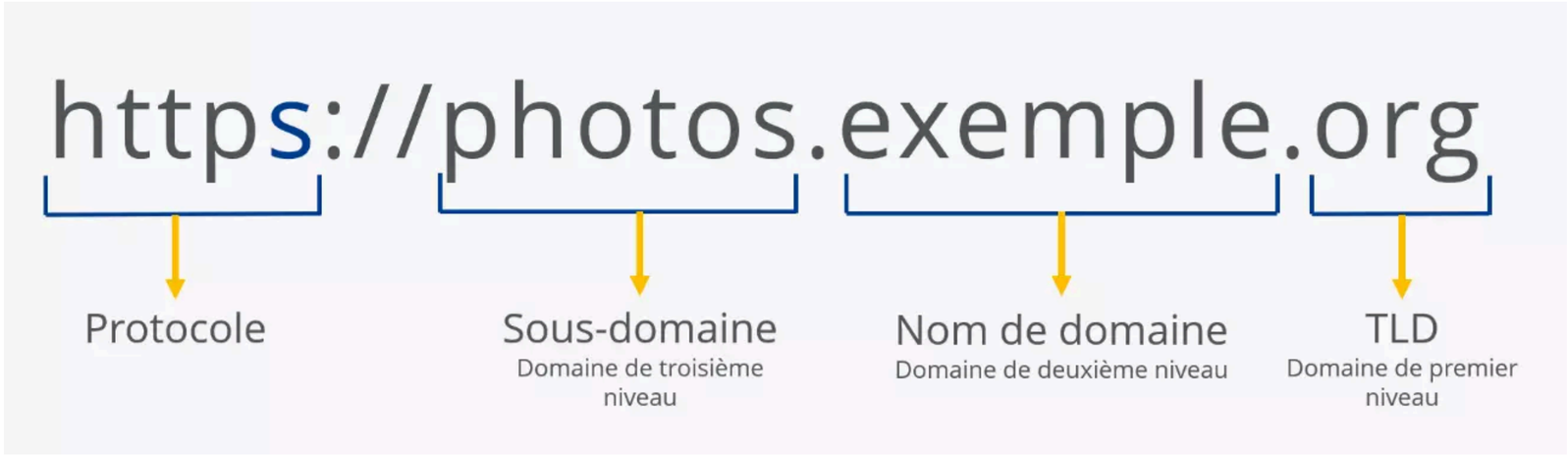
# Phishing

## Comment éviter ce genre de situation ?

1. **Vérifier** l'adresse e-mail (c'est une bonne habitude)
2. L'urgence **inhabituelle** (encore !)
3. La demande inhabituelle (et inédite)
4. L'**orthographe**
5. L'**URL** du lien dans le mail (exemple : un .ru plutôt qu'un .fr)

# Phishing

## Les adresses URL



# Phishing

## Comment repérer un phishing

### Vérifier l'expéditeur

- Inspecter l'adresse e-mail exacte.
- Chercher une adresse suspecte (fautes, domaine étrange).
- Se méfier des expéditeurs inconnus ou inattendus.

### Analyser le contenu du message

- Repérer fautes, langue étrange, mise en forme inhabituelle.
- Attention aux messages urgents ("compte bloqué", etc.).
- Ne jamais donner d'informations personnelles.
- Se méfier des pièces jointes non sollicitées.

### Examiner les liens

- Survoler les liens sans cliquer pour voir l'URL réelle.
- Vérifier que le domaine est officiel.
- Se méfier des liens raccourcis.

# Phishing

## Vérifier les pièces jointes

- Ne pas ouvrir les fichiers inattendus (ZIP, EXE, DOCM…).
- Attention aux fausses factures / colis / banques.

## Éléments techniques

- Vérifier si le mail a été marqué comme spam.
- Pour les utilisateurs avancés : examiner SPF / DKIM / DMARC.

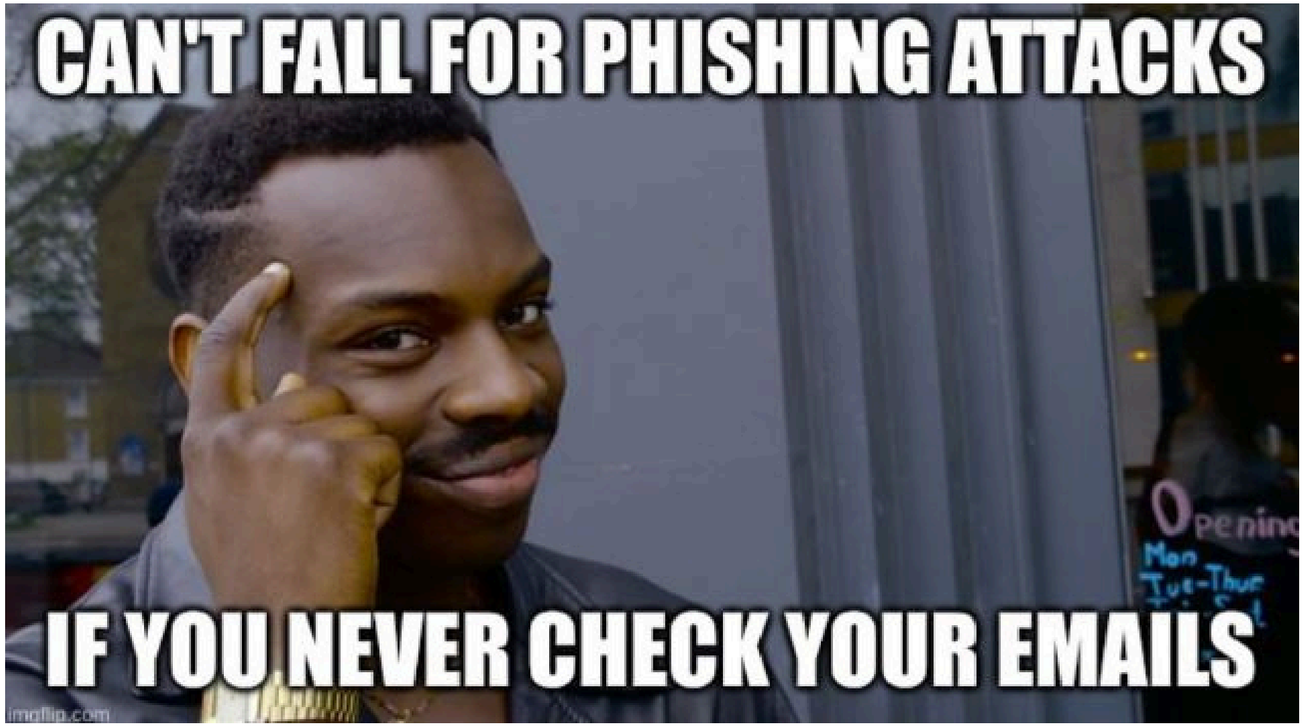
## Utiliser le bon sens

- Vérifier si le message est logique pour vous.
- Confirmer via un autre canal (site officiel, appel…).

## En cas de doute

- Ne pas cliquer.
- Ne pas répondre.
- Ne pas transférer.
- Supprimer ou signaler comme phishing.

# Phishing


CAN'T FALL FOR PHISHING ATTACKS
IF YOU NEVER CHECK YOUR EMAILS
imgflip.com

# Fuite de données

Agathe est une consultante en communication avec des entreprises du CAC 40. Elle se déplace beaucoup, et a toujours son ordinateur portable.

Un vendredi soir, elle s'arrête pour prendre un café. Elle pose son ordinateur sur une chaise, répond à un appel, et se lève pour partir... et oublie son ordinateur.

Elle s'en rend compte 2h plus tard, et l'ordinateur a disparu.

# Fuite de données

## Conséquences

- Rachat du matériel
- Perte de **réputation**
- Amende de 80 000€

Une amende RGPD peut aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire

https://www.cnil.fr/fr/les-sanctions-prononcees-par-la-cnil

# Fuite de données

## RGPD

- **Déclarer** la fuite à la CNIL sous 72 heures
- Prévenir chaque client que leurs données sont **compromises**

https://www.cnil.fr/fr/services-en-ligne/notifier-une-violation-de-donnees-personnelles
https://www.cybermalveillance.gouv.fr/

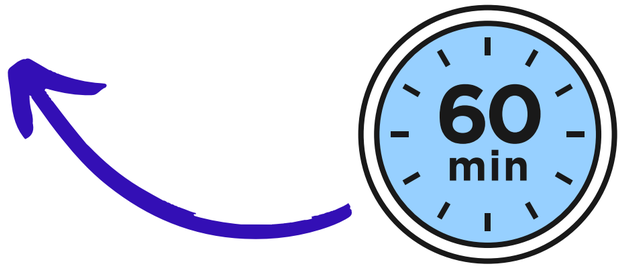
## CNIL

- Organisme qui applique les règles EU
- Objectif : que les entreprises se conforment
- L'amende arrive généralement en cas de non-coopération

# Fuite de données

## Comment éviter ce genre de situation ?

1. **Authentification forte** (un vrai mot de passe, complexe)
2. **Chiffrement** : BitLocker (Windows) ou FileVault (Mac)
3. Sauvegarde **Cloud**
4. Localisation à distance



# Mot de passe complexe

azerty

azerty1234

simone9812!

SimoNE9812!

SimoNE98!Swift12

$SimoNE98!Swift12#Grxlpz

_.E8p%F3+6TZBuib5$yD($TVWL.{)wUY

# En résumé

| Menaces | Conséquences | Signes à repérer et prévention |
|---|---|---|
| **Ransomware** | Fichiers chiffrés, arrêt d'activité (3 semaines), coût 59-100k€ | E-mail inattendu, pièce jointe .zip ou .exe |
| **Phishing** | Vol d'identifiants, piratage de comptes | Urgence, fautes, e-mail suspect |
| **Fuite données** | Amendes RGPD (20M€ / 4% CA), plaintes clients | Chiffrement, sauvegarde, authentification forte |

# Quiz

**Je suis trop petit·e pour être ciblé·e**

Vrai ou faux ?

**J'ai un antivirus, cela me suffit**

Vrai ou faux ?

**La cyberattaque, c'est le problème des informaticiens**

Vrai ou faux ?

# Quiz

## Je suis trop petit·e pour être ciblé·e

Faux ! 60% des attaques ciblent les TPE et le PME.

## J'ai un antivirus, cela me suffit

Faux ! Seulement 25 à 50% des menaces sont détectées.

## La cyberattaque, c'est le problème des informaticiens

Faux ! 95% des attaques ciblent l'erreur humaine.
La cybersécurité, c'est 20% de technique, et 80% de comportement.

# ÉCHANGES DE PRATIQUES

# Scénarios pratiques

| # | Scénario | Risqué ? |
|---|---|---|
| 1 | Lien WeTransfer inattendu | |
| 2 | WiFi public au café | |
| 3 | Mot de passe simple | |
| 4 | Clé USB trouvée | |
| 5 | E-mail urgent patron | |
| 6 | Google Drive public | |
| 7 | Mise à jour reportée | |
| 8 | Mot de passe partagé | |
| 9 | Sauvegarde local | |
| 10 | Télétravail ordi perso | |

# Scénarios pratiques

| # | Scénario | Bon réflexe |
|---|---|---|
| 1 | Lien WeTransfer inattendu | Confirmer par téléphone/SMS |
| 2 | WiFi public au café | |
| 3 | Mot de passe simple | |
| 4 | Clé USB trouvée | |
| 5 | E-mail urgent patron | |
| 6 | Google Drive public | |
| 7 | Mise à jour reportée | |
| 8 | Mot de passe partagé | |
| 9 | Sauvegarde local | |
| 10 | Télétravail ordi perso | |

# Scénarios pratiques

| # | Scénario | Bon réflexe |
|---|---|---|
| 1 | Lien WeTransfer inattendu | Confirmer par téléphone/SMS |
| 2 | WiFi public au café | Utiliser un VPN |
| 3 | Mot de passe simple | |
| 4 | Clé USB trouvée | |
| 5 | E-mail urgent patron | |
| 6 | Google Drive public | |
| 7 | Mise à jour reportée | |
| 8 | Mot de passe partagé | |
| 9 | Sauvegarde local | |
| 10 | Télétravail ordi perso | |

# Scénarios pratiques

| # | Scénario | Bon réflexe |
|---|---|---|
| 1 | Lien WeTransfer inattendu | Confirmer par téléphone/SMS |
| 2 | WiFi public au café | Utiliser un VPN |
| 3 | Mot de passe simple | Min. 12 car. + gestionnaire |
| 4 | Clé USB trouvée | |
| 5 | E-mail urgent patron | |
| 6 | Google Drive public | |
| 7 | Mise à jour reportée | |
| 8 | Mot de passe partagé | |
| 9 | Sauvegarde local | |
| 10 | Télétravail ordi perso | |

# Scénarios pratiques

| # | Scénario | Bon réflexe |
|---|---|---|
| 1 | Lien WeTransfer inattendu | Confirmer par téléphone/SMS |
| 2 | WiFi public au café | Utiliser un VPN |
| 3 | Mot de passe simple | Min. 12 car. + gestionnaire |
| 4 | Clé USB trouvée | NE JAMAIS brancher |
| 5 | E-mail urgent patron | |
| 6 | Google Drive public | |
| 7 | Mise à jour reportée | |
| 8 | Mot de passe partagé | |
| 9 | Sauvegarde local | |
| 10 | Télétravail ordi perso | |

# Scénarios pratiques

| # | Scénario | Bon réflexe |
|---|---|---|
| 1 | Lien WeTransfer inattendu | Confirmer par téléphone/SMS |
| 2 | WiFi public au café | Utiliser un VPN |
| 3 | Mot de passe simple | Min. 12 car. + gestionnaire |
| 4 | Clé USB trouvée | NE JAMAIS brancher |
| 5 | E-mail urgent patron | Confirmer via un autre canal |
| 6 | Google Drive public | |
| 7 | Mise à jour reportée | |
| 8 | Mot de passe partagé | |
| 9 | Sauvegarde local | |
| 10 | Télétravail ordi perso | |

# Scénarios pratiques

| # | Scénario | Bon réflexe |
|---|---|---|
| 1 | Lien WeTransfer inattendu | Confirmer par téléphone/SMS |
| 2 | WiFi public au café | Utiliser un VPN |
| 3 | Mot de passe simple | Min. 12 car. + gestionnaire |
| 4 | Clé USB trouvée | NE JAMAIS brancher |
| 5 | E-mail urgent patron | Confirmer via un autre canal |
| 6 | Google Drive public | Partager nominativement |
| 7 | Mise à jour reportée | |
| 8 | Mot de passe partagé | |
| 9 | Sauvegarde local | |
| 10 | Télétravail ordi perso | |

# Scénarios pratiques

| # | Scénario | Bon réflexe |
|---|---|---|
| 1 | Lien WeTransfer inattendu | Confirmer par téléphone/SMS |
| 2 | WiFi public au café | Utiliser un VPN |
| 3 | Mot de passe simple | Min. 12 car. + gestionnaire |
| 4 | Clé USB trouvée | NE JAMAIS brancher |
| 5 | E-mail urgent patron | Confirmer via un autre canal |
| 6 | Google Drive public | Partager nominativement |
| 7 | Mise à jour reportée | Maximum 1 semaine de délai |
| 8 | Mot de passe partagé | |
| 9 | Sauvegarde local | |
| 10 | Télétravail ordi perso | |

# Scénarios pratiques

| # | Scénario | Bon réflexe |
|---|---|---|
| 1 | Lien WeTransfer inattendu | Confirmer par téléphone/SMS |
| 2 | WiFi public au café | Utiliser un VPN |
| 3 | Mot de passe simple | Min. 12 car. + gestionnaire |
| 4 | Clé USB trouvée | NE JAMAIS brancher |
| 5 | E-mail urgent patron | Confirmer via un autre canal |
| 6 | Google Drive public | Partager nominativement |
| 7 | Mise à jour reportée | Maximum 1 semaine de délai |
| 8 | Mot de passe partagé | Gestionnaire d'équipe |
| 9 | Sauvegarde local | |
| 10 | Télétravail ordi perso | |

# Scénarios pratiques

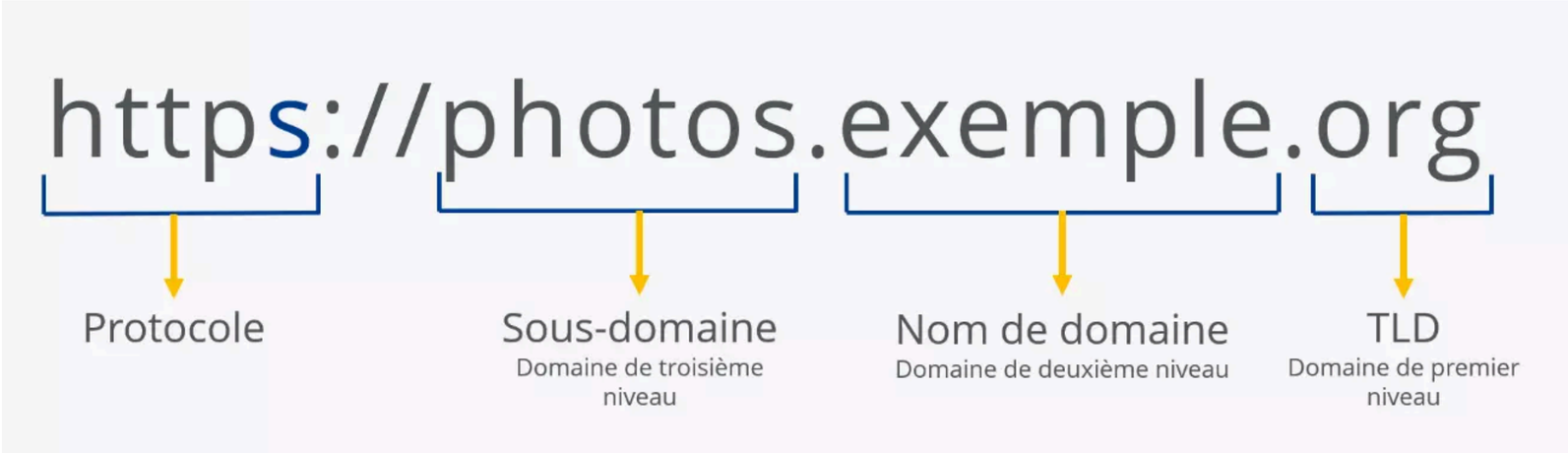
| # | Scénario | Bon réflexe |
|---|---|---|
| 1 | Lien WeTransfer inattendu | Confirmer par téléphone/SMS |
| 2 | WiFi public au café | Utiliser un VPN |
| 3 | Mot de passe simple | Min. 12 car. + gestionnaire |
| 4 | Clé USB trouvée | NE JAMAIS brancher |
| 5 | E-mail urgent patron | Confirmer via un autre canal |
| 6 | Google Drive public | Partager nominativement |
| 7 | Mise à jour reportée | Maximum 1 semaine de délai |
| 8 | Mot de passe partagé | Gestionnaire d'équipe |
| 9 | Sauvegarde local | Règle 3-2-1 |
| 10 | Télétravail ordi perso | |

# Scénarios pratiques

| # | Scénario | Bon réflexe |
|---|---|---|
| 1 | Lien WeTransfer inattendu | Confirmer par téléphone/SMS |
| 2 | WiFi public au café | Utiliser un VPN |
| 3 | Mot de passe simple | Min. 12 car. + gestionnaire |
| 4 | Clé USB trouvée | NE JAMAIS brancher |
| 5 | E-mail urgent patron | Confirmer via un autre canal |
| 6 | Google Drive public | Partager nominativement |
| 7 | Mise à jour reportée | Maximum 1 semaine de délai |
| 8 | Mot de passe partagé | Gestionnaire d'équipe |
| 9 | Sauvegarde local | Règle 3-2-1 |
| 10 | Télétravail ordi perso | Session séparée |

# Précisions

## Les adresses URL




## HTTP et HTTPS

Avec HTTPS, le contenu envoyé au navigateur est chiffré

## Règle 3-2-1

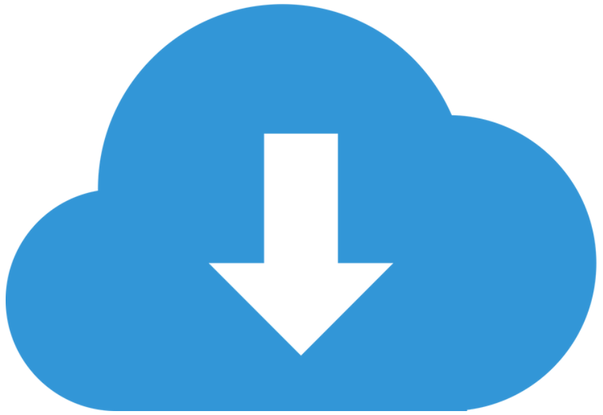
- 3 copies
- 2 support
- 1 hors-site

# Questions ouvertes

## Avez-vous déjà eu un doute sur un e-mail reçu ?

# Questions ouvertes

## Qui sauvegarde régulièrement ses fichiers ?



# SOLUTIONS
# &
# FEUILLES DE ROUTE

—

Programme sur 3 mois

# Premier mois

Les fondations

## Priorité : Mots de passe et authentification

Semaine 1 et 2

| | |
|---|---|
| **Action** | Installer un gestionnaire de mots de passe |
| **Outils** | Bitwarden (gratuit, open source) ou KeePassXC (local) |
| **Temps** | 1 heure |

- Choisir et installer le gestionnaire
- Créer un mot de passe maître fort (phrase de 20+ caractères)
- Identifier vos 5 comptes les plus critiques
- Générer et sauvegarder 5 nouveaux mots de passe forts

# Premier mois

Les fondations

## Priorité : Mots de passe et authentification

Semaine 3 et 4

| | |
|---|---|
| **Action** | Activer la double authentification (2FA) |
| **Outils** | Google Authenticator, Microsoft Authenticator, Authy |
| **Temps** | 30 minutes |

- Installer une application d'authentification
- Activer 2FA sur votre e-mail professionnel
- Activer 2FA sur 3 services critiques (banque, cloud, etc.)
- Configurer une sauvegarde cloud automatique (Google Drive, pCloud, etc.)
- Tester la restauration d'un fichier

# Deuxième mois

La consolidation

## Priorité : Mises à jour et sensibilisation

Semaine 5 et 6

| | |
|---|---|
| **Action** | Mettre en place les mises à jour automatiques |
| **Outils** | Votre OS |
| **Temps** | 30 minutes |

- Activer mises à jour auto (Windows Update ou macOS)
- Planifier 1h/semaine pour les mises à jour manuelles
- Mettre à jour : navigateurs, suite Office, PDF, antivirus
- Règle : ne jamais reporter plus d'1 semaine

# Deuxième mois

La consolidation

## Priorité : Mises à jour et sensibilisation

Semaine 7 et 8

| | |
|---|---|
| **Action** | Organiser une mini-formation phishing en équipe |
| **Outils** | Vous-même 🙂 |
| **Temps** | 1 heure |

- Créer une checklist "Comment repérer un phishing"
- Organiser 1h de sensibilisation avec toute l'équipe
- Instaurer la règle : "En cas de doute, on partage"

# Troisième mois

L'optimisation

## Priorité : Sécurisation réseau et gestion des accès

Semaine 9 et 10

| | |
|---|---|
| **Action** | Sécuriser le WiFi professionnel et installer un VPN |
| **Outils** | ProtonVPN (gratuit, illimité) ou Windscribe (10 Go/mois) |
| **Temps** | 1 heure |

- Changer le mot de passe Wi-Fi par défaut de la box
- Activer le chiffrement WPA3 (ou WPA2 minimum)
- Installer un VPN sur tous les appareils mobiles
- Tester le VPN sur un réseau public

# Troisième mois

L'optimisation

## Priorité : Sécurisation réseau et gestion des accès

Semaine 11 et 12

| | |
|---|---|
| **Action** | Créer la procédure de gestion des accès |
| **Outils** | Votre équipe ! |
| **Temps** | 2 heure |

- Créer un tableau des accès (qui a accès à quoi)
- Faire l'audit des droits d'accès actuels
- Rédiger une checklist de départ collaborateur
- Premier nettoyage de données (supprimer les données obsolètes qui ont plus de 2 ans, notamment celles des clients)
- Documenter les durées de conservation

# Après les 3 mois

Amélioration continue

## Actions trimestrielles

- Mini-formation phishing (30 min)
- Nettoyage de données (2h)
- Révision des accès

## Actions annuelles

- Changement mots de passe critiques
- Audit complet des droits d'accès
- Test de restauration des sauvegardes
- Évaluation cyber-assurance (300 à 500€)

## Actions hebdomadaires

- Mises à jour (30 min)
- Vérification des sauvegardes

# Après les 3 mois

Amélioration continue

## Félicitations !

## Vous avez significativement réduit vos risques !

# Checklist d'auto-diagnostic

# RESSOURCES & TUTORIELS

# Outils gratuits

| Gestionnaires de mots de passe | |
|---|---|
| **Bitwarden** | https://bitwarden.com<br>Gratuit, open source, synchronisation cloud |
| **KeePassXC** | https://keepassxc.org<br>Gratuit, local (pas de cloud), très sécurisé |
| **Applications d'authentification (2FA)** | |
| **Google Authenticator** | Gratuit, iOS et Android |
| **Microsoft Authenticator** | Gratuit, iOS et Android, sauvegarde cloud |
| **Authy** | https://authy.com<br>Multi-appareils |

# Outils gratuits

| Sauvegardes cloud | |
|---|---|
| **Google Drive** | 15 Go gratuit, intégration Google Workspace |
| **pCloud** | 10 Go gratuit, chiffrement disponible |
| **Sync.com** | 5 Go gratuit, chiffrement de bout en bout |
| **VPN gratuits fiables** | |
| **ProtonVPN** | https://protonvpn.com<br>Gratuit illimité, Suisse, pas de logs |
| **Windscribe** | https://windscribe.com<br>10 Go/mois gratuit |

# Outils gratuits

| Antivirus gratuits | |
|---|---|
| **Windows Defender** | Intégré à Windows, activé par défaut |
| **Avast Free** | https://www.avast.com |
| **AVG Free** | https://www.avg.com |

# Sites de formation et sensibilisation

| ANSSI - Agence Nationale de la Sécurité des SI | |
|---|---|
| **Guides** | https://www.ssi.gouv.fr/guides<br>Guides gratuits par thématique |
| **Formation** | SecNumAcadémie - MOOC gratuit (12h) |
| **Cybermalveillance.gouv.fr** | |
| **Site** | https://www.cybermalveillance.gouv.fr |
| **Services** | Assistance en cas d'attaque<br>Fiches pratiques par menace<br>Diagnostic en ligne gratuit |
| **CNIL - Pour le RGPD** | |
| **Guide TPE/PME** | https://www.cnil.fr/fr/rgpd-passer-a-laction |
| **Services** | Modèles de registres, procédures, lettres |

# Tester vos connaissances

| | |
|---|---|
| **Quiz phishing** | Google Phishing Quiz<br>https://phishingquiz.withgoogle.com<br>Test gratuit et ludique en 5 minutes |
| **Solidité mots de passe** | How Secure Is My Password<br>https://howsecureismypassword.net<br>⚠️ Ne pas entrer vos vrais mots de passe ! |
| **Fuites de données** | Have I Been Pwned<br>https://haveibeenpwned.com<br>Vérifiez si vos données ont fuité |

# Contacts utiles

| En cas de cyberattaque | |
|---|---|
| **URGENCE** | ☎ 0 805 805 817 |
| **Cybermalveillance** | https://www.cybermalveillance.gouv.fr<br>Plateforme d'assistance<br>Gratuit, disponible 24/7 |
| **Police/Gendarmerie** | Dépôt de plainte (obligatoire pour assurance) |
| **Pour le RGPD** | |
| **CNIL** | ☎ 01 53 73 22 22<br>https://www.cnil.fr |
| **Signaler un contenu illicite** | |
| **Pharos** | https://www.internet-signalement.gouv.fr<br>Plateforme officielle de signalement |

# CONCLUSION

# Ressources et tutoriels

| Catégorie | Outils / Liens |
|---|---|
| **Mots de passe** | Bitwarden (gratuit), KeePassXC (local) |
| **2FA** | Google Authenticator, Microsoft Authenticator, Authy |
| **Cloud** | Google Drive (15 Go), pCloud, Sync.com |
| **VPN** | ProtonVPN (illimité), Windscribe (10 Go/mois) |
| **Formation** | ANSSI, Cybermalveillance.gouv.fr, CNIL |
| **Urgence** | 0 805 805 817 - Cybermalveillance.gouv.fr |
| **RGPD** | CNIL : 01 53 73 22 22 |

## La cybersécurité n'est pas un état, c'est un chemin.

Vous n'avez pas besoin d'être parfaits dès demain, mais d'avancer **progressivement**.

Les 3 messages clefs :

1. Vous êtes une cible - Les hackers ne font pas de distinction
2. 80% = **comportement** - Votre vigilance fait la différence
3. Agissez progressivement - Mois par mois, sans pression

# Et vous, quelle sera votre première action ?

IT security in 1990s

Memes
@memes

Laugh all you want, but the information on those floppies can't be hacked from half a world away

# MERCI !