PROTÉGEZ-VOUS DES CYBERCRIMINELS

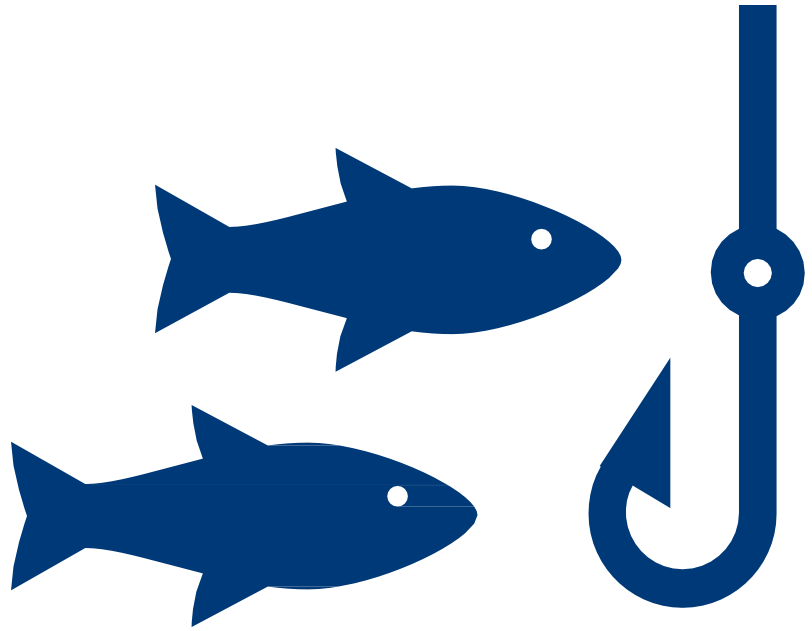
INTRODUCTION AUX BONNES PRATIQUES ESSENTIELLES POUR LES TPE,
ARTISANS, COMMERÇANTS
ET PROFESSIONNELS LIBÉRAUX.

LES TYPES DE CYBERMENACES COURANTES :

- Le phishing (Hameçonnage)
- Le spear phishing (Hameçonnage ciblé)
- Le vishing (Hameçonnage vocal)

LE PHISHING OU HAMEÇONNAGE

Le phishing (ou hameçonnage en français) est une méthode utilisée par les cybercriminels qui consister à imiter une entité de confiance (banque, fournisseur, administration….)
afin de récupérer des informations sensibles (mots de passe, coordonnées bancaires…).



Le phishing – Quelques exemples

PeyPal

Accès fraduleux

Bonjour,

Nous avons interdit l'accès à votre compte pour la raison suivante.
Votre dernière tentative de connexion a échoué depuis l'adresse IP suivante :
9 rue des cerisiers, 75100, Paris, Île-de-France
Pour être sur que vos informations restent protégées contre les menaces, cliquez sur le bouton "Vérifier mon compte"

Chez PayPal, votre sécurité est notre priorité absolue.

Vérifier mon compte

Le phishing – Quelques exemples

Logo d'une entité de confiance imité

Informations poussant la cible à l'action

Lien malveillant

Le phishing – Quelques exemples

Cdiscount
Expéditeur : cdiscount.noreply@factory.de
À : cadeau@cdscount.com

Cdiscount

Aujourd'hui, Vous avez été sélectionné parmi nos clients

pour gagner une carte cadeau d'une valeur de 1000€ chez Cdiscount!

Pour recevoir votre cadeau, il vous suffit de renseigner les informations

Dont votre adresse E-mail, Numéro de Téléphone, Adresse...

Sélectionnez et gagnez mon cadeau

*Offre valable jusqu'au 31 Mars 2024 inclus, limitée aux 1 000 premiers gagnant(e)s.

Le phishing – Quelques exemples

Le phishing – Les Risques

Cas concret :

Un cybercriminel imite l'interface de votre banque et récupère l'accès à vos comptes.

Un cybercriminel imite l'interface de votre boîte mail et communique un nouveau RIB à vos clients.

- Perte financière
- Vol de données sensibles
- Infection de votre appareil
- Atteinte à l'image et perte de confiance

QUIZ 1 : LE PHISHING – LES RISQUES

Les banques vous remboursent systématiquement en cas d'arnaques subies :

Réponse A :	**Réponse B :**
Vrai	Faux

REPONSE QUIZ 1 : LE PHISHING – LES RISQUES

Les banques vous remboursent systématiquement en cas d'arnaques subies :

Réponse A :	**Réponse B :**
Vrai	Faux

Le phishing – Les Risques

La responsabilité de l’entreprise :

En cas de négligence (ex : mauvais contrôle des paiements, absence de double vérification), la banque peut refuser de rembourser les dommages.

La Cour de cassation confirme que, si l’entreprise n’a pas pris les précautions nécessaires, elle assume seule la perte.

Arnaque : la banque n’est pas tenue de rembourser la victime négligente

Publié le 07 mars 2025 - Direction de l'information légale et administrative (Premier ministre)

La victime d’une escroquerie ne peut pas obtenir un remboursement de la banque si elle a fait preuve de négligence. C’est ce que la Cour de cassation indique dans un arrêt rendu le 15 janvier 2025 et publié au bulletin.

Crédits: fizkes - stock.adobe.com

Deux sociétés ont subi une attaque informatique par hameçonnage ayant conduit au versement de 6 virements vers des comptes étrangers. Elles ont demandé, sans succès, à leur banque le remboursement de ces opérations de paiement non autorisées. Elles saisissent la justice et assignent la banque en remboursement.

La cour d’appel condamne la banque à rembourser les sociétés à hauteur de 50 % des pertes subies. Pour elle, la banque a manqué à ses obligations de vigilance et de surveillance de ses systèmes. La banque se pourvoit en cassation.

La Cour de cassation casse et annule l’arrêt rendu en appel. Elle soutient que la responsabilité de la banque n’a pas été retenue par la cour d’appel en raison de la négligence des sociétés clientes. Ainsi, **seules celles-ci doivent supporter les pertes subies**.

Ainsi, la banque n’a pas à rembourser son client victime d’une escroquerie bancaire **lorsque celui-ci a commis une négligence grave**.

Le phishing – Les Risques

Cas concret :

Un cybercriminel imite l'interface d'un site internet et vole vos identifiants.

Un cybercriminel imite l'interface de votre stockage en ligne et accède à tous vos fichiers.

- Perte financière
- Vol de données sensibles
- Infection de votre appareil
- Atteinte à l'image et perte de confiance

Le phishing – Les Risques

Cas concret :

Un cybercriminel installe un logiciel malveillant sur votre ordinateur / téléphone en vous faisant cliquer sur un lien ou une pièce jointe.

- Perte financière
- Vol de données sensibles
- Infection de votre appareil
- Atteinte à l'image et perte de confiance

Le phishing – Les Risques

Cas concret :

Un cybercriminel arrive à prendre le contrôle de votre boîte mail, et va ensuite l'utiliser pour pirater vos clients.

- Perte financière
- Vol de données sensibles
- Infection de votre appareil
- Atteinte à l'image et perte de confiance

Le phishing – Comment le détecter

Vérifier l'expéditeur :

- Mail, domaine, affichage trompeur…

Analyser le contenu du message :

- Fautes, urgence et pression psychologique, tonalité utilisée…

Inspecter les liens et pièces jointes

- Survoler le lien pour regarder, affichage trompeur…

Vérifier l'authenticité par un autre canal de communication

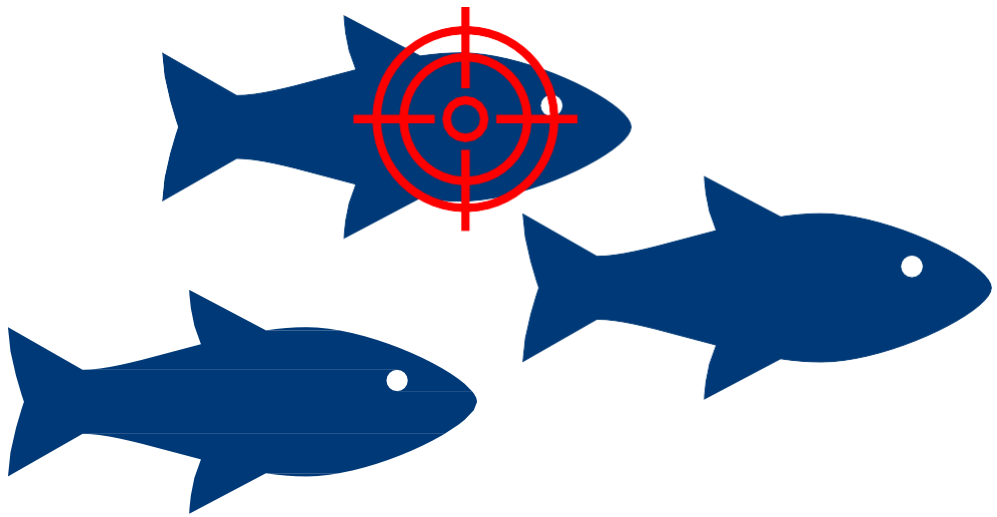
- Si vous avez un doute, contactez la personne par téléphone, sms…

Faire preuve de bon sens et d'humilité

- On ne gagne jamais un concours auquel on n'a pas participé
- Le meilleur moyen de se faire pirater c'est de penser qu'on ne peut pas se faire pirater

LE SPEAR PHISHING

Contrairement au phishing classique, qui envoie des emails en masse de façon aléatoire, le spearphishing (hameçonnage ciblé en français) vise une personne ou une entreprise spécifique en utilisant des informations précises (nom, fonction, partenaires, habitudes) pour rendre l'attaque plus crédible.



LE SPEAR PHISHING – UN EXEMPLE

Quelques informations :

- Vous êtes Jérôme, président d'une TPE.
- Vous êtes client du cabinet comptable : Expertcompta.
- La comptable qui gère votre dossier et avec qui vous êtes régulièrement en contact s'appelle Myriame.

Comment ces informations peuvent être obtenues :

- Internet (réseaux sociaux, fuite de données…).
- Phishing…
- Mentions légales C bases de données publiques…
- Personne qui vous observe ou vous écoute dans des lieux publics…

LE SPEAR PHISHING – UN EXEMPLE

[URGENT] Régularisation DGFIP – Cotisation Fiscale en attente

JD Jean.dupont@cabinet-experlcompta.com
À Vous

Bonjour Jérôme,

J'espère que vous allez bien.

Je remplace Myriame en son absence en cette fin de semaine.

Je viens d'être contacté par la DGFIP, le Service Recouvrement Professionnels, qui m'informe que votre entreprise a un solde à régulariser de 3 248,56 € pour la cotisation foncière des entreprises (CFE) 2023.

Après vérification, cette somme n'a pas été prélevée en raison d'un retard de traitement. Afin d'éviter des pénalités, je vous recommande d'effectuer le règlement avant demain.

- Montant dû : 3 248,56 €
- Référence dossier : 2025-CFE-27001
- Bénéficiaire : DGFIP – Recouvrement Professionnels
- IBAN : FR76 1234 5678 9012 3456 7890 123
- BIC : TRSDFRPPXXX

Vous pouvez effectuer ce virement directement depuis votre banque. Merci de me transmettre la confirmation une fois le paiement réalisé, afin que je mette à jour la comptabilité et informe la DGFIP du règlement. Merci de bien vouloir traiter ce paiement **avant la fin de journée** afin d'éviter des pénalités de retard. Vous pouvez me contacter directement au **06 XX XX XX XX** en cas de besoin.

Bien cordialement,

Jean Dupont
Expert-Comptable | Cabinet ExpertCompta France
06 XX XX XX XX | j.dupont@expertcompta-france.com
12 Rue des Malveillants, 75008 Paris

LE SPEAR PHISHING – UN EXEMPLE

[URGENT] Régularisation DGFIP – Cotisation Fiscale en attente

JD Jean.dupont@cabinet-experlcompta.com
À Vous

Bonjour Jérôme,

J'espère que vous allez bien.

Je remplace Myriame en son absence en cette fin de semaine.

Je viens d'être contacté par la DGFIP, le Service Recouvrement Professionnels, qui m'informe que votre entreprise a un solde à régulariser de 3 248,56 € pour la cotisation foncière des entreprises (CFE) 2023.

Après vérification, cette somme n'a pas été prélevée en raison d'un retard de traitement. Afin d'éviter des pénalités, je vous recommande d'effectuer le règlement avant demain.

- Montant dû : 3 248,56 €
- Référence dossier : 2025-CFE-27001
- Bénéficiaire : DGFIP – Recouvrement Professionnels
- IBAN : FR76 1234 5678 9012 3456 7890 123
- BIC : TRSDFRPPXXX

Vous pouvez effectuer ce virement directement depuis votre banque. Merci de me transmettre la confirmation une fois le paiement réalisé, afin que je mette à jour la comptabilité et informe la DGFIP du règlement. Merci de bien vouloir traiter ce paiement **avant la fin de journée** afin d'éviter des pénalités de retard. Vous pouvez me contacter directement au **06 XX XX XX XX** en cas de besoin.

Bien cordialement,

Jean Dupont
Expert-Comptable | Cabinet ExpertCompta France
06 XX XX XX XX | j.dupont@expertcompta-france.com
12 Rue des Malveillants, 75008 Paris

Le spear phishing – Comment le détecter

Vérifier l'expéditeur :
- Mail, domaine, affichage trompeur…

Analyser le contenu du message :
- Fautes, urgence et pression psychologique, tonalité utilisée…

Inspecter les liens et pièces jointes
- Survoler le lien pour regarder, affichage trompeur…

Vérifier l'authenticité par un autre canal de communication
- Si vous avez un doute, contactez la personne par téléphone, sms…

Faire preuve de bon sens et d'humilité
- Le meilleur moyen de se faire pirater c'est de penser qu'on ne peut pas se faire pirater

LE VISHING

Contrairement au phishing par email, le vishing (hameçonnage vocal) utilise des appels téléphoniques ciblés.

L'attaquant se fait passer pour un contact de confiance afin d'obtenir des informations sensibles ou de pousser la victime à une action frauduleuse.

Le vishing – Comment le détecter

- **Urgence et pression** : L'interlocuteur, souvent une femme pour attiser la confiance, insiste sur une action immédiate (paiement, changement de mot de passe…).

- **Fonction usurpée**: Il prétend souvent être un banquier, un support technique, un organisme officiel…

- **Demande d'informations ou d'actions sensibles** : Mot de passe, numéro de carte bancaire, accès à un compte…

- **Numéro masqué ou inconnu** : Attention aux appels provenant de numéros inhabituels.

Le bon réflexe : raccrocher et rappeler par vous même l'organisme

LES BASES DE LA CYBERSÉCURITÉ :

- Les mots de passe
- La double authentification

Mots de passe - Les mauvaises habitudes

Dates :	Année de naissance (1968,1983,2000…) Date d'evenement important (mariage, diplomation…)
Noms /prénoms :	Prenom des enfants (Emma2002, Jules 2012…) Nom du conjoint (Pauline1988, Jean1992…) Nom d'un annimal (rex123, Petitchat83130…)
Habitude fréquentes :	Ville de résidence (Laciotat13600, Lyon69…) Les passions (Michaeljackson, OM1993…)
Variantes ultra classiques :	Caractère spécial à la fin et la première lettre en majuscule (Rex123@, Toutou83!...) Les mots de passes classiques (0000, 2025, azerty123, Admin, 1234….)

QUIZ 2 : MOTS DE PASSE – LA RÉSISTANCE

Combien de temps faudrait-il à un cybercriminel pour forcer le mot de passe suivant : **Leo99**

Réponse A : Instantané	**Réponse B :** 6 Secondes
Réponse C : 2 Heures	**Réponse D :** 3 Ans

REPONSE QUIZ 2 : MOTS DE PASSE – LA RÉSISTANCE

Combien de temps faudrait-il à un cybercriminel pour forcer le mot de passe suivant : **Leo99**

Réponse A : Instantané	**Réponse B :** 6 Secondes
Réponse C : 2 Heures	**Réponse D :** 3 Ans

Mots de passe – La résistance

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Immédiat	Immédiat	3 secs	6 secs	9 secs
5	Immédiat	4 secs	2 mins	6 mins	10 mins
6	Immédiat	2 mins	2 heures	6 heures	12 heures
7	4 secs	50 mins	4 jours	2 semaines	1 mois
8	37 secs	22 heures	8 mois	3 ans	7 ans
9	6 mins	3 semaines	33 ans	161 ans	479 ans
10	1 heure	2 ans	1k ans	9k ans	33k ans
11	10 heures	44 ans	89k ans	618k ans	2M ans
12	4 jours	1k ans	4M ans	38M ans	164M ans
13	1 mois	29k ans	241M ans	2Md ans	11Md ans
14	1 an	766k ans	12Md ans	147Md ans	805Md ans
15	12 ans	19M ans	652Md ans	9Bn ans	56Bn ans
16	119 ans	517M ans	33Bn ans	566Bn ans	3qd ans
17	1k ans	13Md ans	1qd ans	35qd ans	276qd ans
18	11k ans	350Md ans	91qd ans	2qn ans	19qn ans

Mots de passe – Les gestionnaires

Un gestionnaire de mots de passe, c'est un coffre-fort numérique sécurisé qui stocke et génère des mots de passe complexes pour vous.

Les intérêts :

- Application très sécurisée
- Un seul mot de passe à retenir
- Permets d'avoir des mots de passe différents pour chaque compte
- Permets de générer des mots passés très complexes
- Complétion automatique des champs

Exemples de mots de passe robuste générés par Proton :

M0!SjqBK1*spbjEzX!^dwrzj!wEbvtX4 (version très robuste)

Passable2-Cupcake3-Neatness4-Armrest3-Abridge1 (version facile à recopier)

LA DOUBLE AUTHENTIFICATION

C’est une protection supplémentaire qui ajoute une deuxième vérification pour se connecter à un compte.

En plus de votre mot de passe, il vous faudra :

- Un code reçu par sms
- Une empreinte digitale ou reconnaissance faciale
- Un code reçu par mail
- Une clé de sécurité physique

Sur quels site, logiciel ou plateforme je dois l’activer ?

- Les comptes critiques (Messageries, réseaux sociaux, outils professionnels…)

LA PROTECTION DES DONNES SENSIBLES

- C’est quoi une donnée sensible ?
- La sauvegarde régulière des données
- Le stockage sécurisé des données clients et financières

LA PROTECTION DES DONNES SENSIBLES

Ce sont les informations qui, si elles sont volées ou perdues, peuvent causer un dommage à l'entreprise ou aux clients !

Quelques exemples :

- **Données clients** : noms, prénoms, emails, numéros de téléphone, adresses…
- **Données financières** : IBAN, RIB, factures, relevés bancaires…
- **Données professionnelles** : devis, contrats, fournisseurs, fichiers internes…
- **Données d'accès** : identifiants, mots de passe, accès aux outils pros…

Pourquoi ces données sont-elles prisées des cybercriminels :

- Les revendre
- Usurpation d'identité
- Mener des attaques ciblées (spearphishing…)
- …

LA PROTECTION DES DONNES SENSIBLES – RGPD

Le **R**ègleme**n**t **G**énéral sur la **P**rotection des **D**onnées est une loi européenne qui encadre l'utilisation des données personnelles.

Pourquoi c'est important ?

- C'est une obligation légale
- Conserver la confiance de vos clients
- Éviter les sanctions de la CNIL

Guide de sensibilisation au RGPD : *bpi-cnil-rgpd_guide-tpe-pme.pdf*

LE STOCKAGE DE VOS DONNÉES

Comment stocker les données de son entreprise :

- **Sur un serveur ou un NAS sécurisé** (idéal pour une équipe interne).
- **Dans un cloud professionnel** (OneDrive, Dropbox Business…).
- **Sur un disque dur externe chiffré** pour les sauvegardes.

⚠ A Éviter :

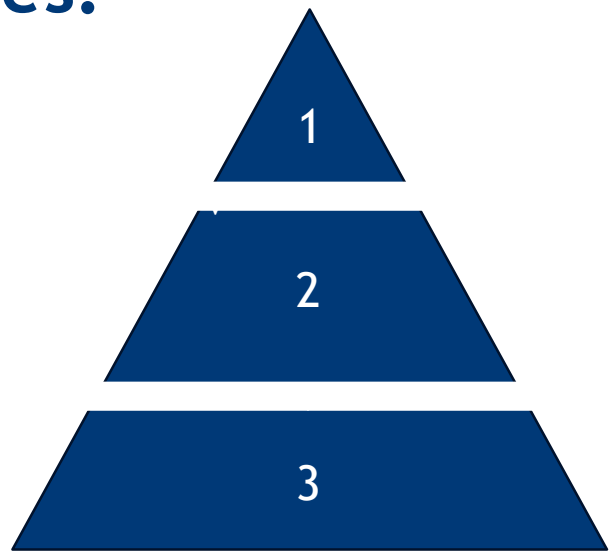
- Le stockage sur des **clés USB non sécurisées.**
- Le stockage sur des **PC personnels.**
- L'usage de **services cloud gratuits non adaptés aux entreprises.**

LA SAUVEGARDE DE VOS DONNÉES

Qu'est-ce qu'il se passerait si vous perdiez accès à toutes vos données ?

Nous sommes tous vulnérables aux **cyberattaques, pannes, erreurs humaines** ou **incendies.** Une sauvegarde permet de **récupérer ses données.**

La règle du 3 – 2 – 1 :



Sauvegarde hors site

Supports différents

Copies des données

LA SAUVEGARDE DE VOS DONNÉES

Un exemple de comment l'appliquer :

3 Copies des données ⟶ l'originale + 2 sauvegardes

2 Supports différents ⟶ Disque dur externe chiffré + cloud

1 Sauvegarde hors site ⟶ Sauvegarde sur le Cloud

LES BONNES PRATIQUES

- La sécurité des WIFI – Votre WIFI
- La sécurité des WIFI - Les réseaux auxquels vous vous connectez
- Sécurisez vos appareils – Vos ordinateurs
- D’autres bonnes pratiques

LA SÉCURITÉ DES WIFI – VOTRE WIFI

Votre réseau WIFI est une porte d'entrée potentielle pour les cybercriminels.

Les bonnes pratiques essentielles pour sécuriser votre réseau WIFI :

- Changer le mot de passe par défaut.
- Désactiver la diffusion du SSID (nom du réseau visible).
- Créer un réseau WIFI pour les invités.
- Ne pas connecter des équipements non sécurisés (vielle imprimante, aspirateur robot, objets connectés…).
- Effectuer régulièrement des mises à jour.
- Installer un Pare-feu si il n'est pas intégré dans votre box.

QUIZ 3 : LA SÉCURITÉ DES WIFI – LES WIFI PUBLICS

Se connecter à un WIFI public représente un risque cyber :

Réponse A :	**Réponse B :**
Vrai	Faux

REPONSE QUIZ 3 : LA SÉCURITÉ DES WIFI – LES WIFI PUBLICS

Se connecter à un WIFI public représente un risque cyber :

Réponse A :	**Réponse B :**
Vrai	Faux

LA SÉCURITÉ DES WIFI – LES WIFI PUBLICS

Se connecter à un Wi-Fi public, c'est comme entrer chez un inconnu et sans connaître les personnes déjà présentes.

Le risque principal : un cybercriminel imite un WIFI public et réalise une attaque « Man-in-the-Middle ».

Une personne s'interpose entre votre ordinateur et internet et intercepte vos données.

LA SÉCURITÉ DES WIFI – LES WIFI PUBLICS

Les bonnes pratiques lorsque vous vous connectez sur un réseau WIFI public :

- Utiliser un VPN pour chiffrer la connexion.
- Éviter d'effectuer des opérations sensibles (paiements, accès aux applications critiques…).
- Privilégier un partage de connexion mobile (4G / 5G) au lieu d'utiliser un WIFI externe.

Sécurisez vos appareils – Vos ordinateurs

Quelques bonnes pratiques pour sécuriser vos ordinateurs :

- Mises à jour de votre OS (Windows, MacOS…), de vos applications, de vos navigateurs… Activez les mises à jour automatiques si possible.
- Chiffrez votre ordinateur, cela permet d'éviter que quelqu'un puisse accéder à vos informations s'il détient votre poste.
- Utilisez un Antivirus.
- Ne téléchargez pas de logiciels peu réputés ou que vous ne connaissez pas.
- Évitez de brancher des périphériques qui ne sont pas à vous sur des ports USB.

D'AUTRES BONNES PRATIQUES

- Ne jamais laisser un ordinateur portable ou une tablette visible dans un véhicule. Le ranger dans le coffre **avant** le départ.

- Mettre en veille avec mot de passe dès qu'on quitte son poste, même pour quelques minutes.

- Utiliser un filtre de confidentialité sur l'écran pour éviter les regards indiscrets
(surtout dans les cafés, trains, salons professionnels).

- Faire attention aux conversations téléphoniques : ne pas donner d'informations
sensibles en public.

- Ne pas noter les mots de passe sur un post-it collé à l'écran ou sur le comptoir.

PRÉPAREZ-VOUS EN CAS D'INCIDENT

- L'importance de s'être préparé à un incident
- Anticiper sa réponse à un incident

L'IMPORTANCE DE S'ÊTRE PRÉPARÉ À UN INCIDENT

En cas d'incident de sécurité, il est primordial d'avoir anticipé une « stratégie » à mettre en place pour :

- Limiter les pertes (financières, réputation…).
- Réagir beaucoup plus rapidement.
- Éviter la panique et les mauvaises décisions.
- Éviter que l'évènement se reproduise.

ANTICIPER SA RÉPONSE À UN INCIDENT

Lister les contacts essentiels en cas d'attaque :

- Votre prestataire informatique ou un expert en cybersécurité identifié en amont.

- cybermalveillance.gouv.fr pour :
  - Effectuer un diagnostic en ligne
  - Trouver un prestataire spécialisé
  - Accéder à des conseils

- Votre banque, à contacter le plus rapidement en cas de fraude.

- Votre assurance.

- Les autorités :
  - La police / gendarmerie.
  - La CNIL en cas de fuite de données.

ANTICIPER SA RÉPONSE À UN INCIDENT

Les premiers gestes :

1. Alertez immédiatement votre support informatique si vous en disposez afin qu'il prenne en compte l'incident (service informatique, prestataire, personne en charge).
2. Débranchez la machine d'internet ou du réseau informatique : Débranchez le câble réseau et désactivez la connexion Wi-Fi ou les connexions de données pour les appareils mobiles.
3. N'éteignez pas l'appareil : Certains éléments de preuve contenus dans la mémoire de l'équipement et nécessaires aux investigations seront effacés s'il est éteint.
4. N'utilisez plus l'équipement potentiellement compromis : Ne touchez plus à l'appareil pour éviter de supprimer des traces de l'attaque utiles pour les investigations à venir.
5. Prévenez vos collègues de l'attaque en cours : Une mauvaise manipulation de la part d'un autre collaborateur pourrait aggraver la situation.

RESSOURCES ET OUTILS

Gestionnaires de mots de passe :

- ProtonPass
- KeePass
- LockPass

Double authentification ;

- Authentificator
- 2FAS

Antivirus :

- Windows Defender
- Avast FREE
- ESET

Solution de chiffrement

- BitLocker

RESSOURCES ET OUTILS

Cybermalveillance (https://www.cybermalveillance.gouv.fr/) :	Diagnostics et conseils pour les entreprises Liste de prestataires de cybersécurité Guides pratiques et fiches réflexes
CNIL (https://www.cnil.fr/fr) :	Informations sur la protection des données personnelles Fiches pratiques pour la mise en conformité au RGPD
Have I been powned (https://haveibeenpwned.com/) :	Vérifier si une adresse mail apparaît dans une fuite de donnée
Virus total (https://www.virustotal.com/gui/home/upload) :	Vérifier des pièces jointes ou des liens
ANNSI (https://cyber.gouv.fr/bonnes-pratiques-protegez-vous) :	Les bonnes pratiques Beaucoup d'informations à destination des TPE / PME

A VOS QUESTIONS !