LES BASES DE LA CYBERSÉCURITÉ

version 1.2 - avril 2026

CONTEXTE, VECTEURS, ATTAQUES ET BONNES PRATIQUES

la ligue de l'enseignement
un avenir par l'éducation populaire

PRÉSENTATION ET DÉFINITIONS

QU'EST-CE QUE LA MENACE CYBER ?

- **Des attaquants :** individuels, groupes organisés, organisations paraétatiques

- **Des objectifs d'attaque :**
  - Lucratifs : vol d'argent, extorsion et demande de rançons
  - Atteinte à l'image
  - Sabotage/espionnage
  - Dégradations
  - Idéologiques ou de déstabilisation

- **Des cibles :** services publics, entreprises et associations de toutes tailles, particuliers

- **Différentes techniques et vecteurs d'attaque**

CONTEXTE ACTUEL EN FRANCE

Cartographie prospective des risques de l'assurance en 2024 :

- N°1 : Cyberattaques
- N°2 : Dérèglement climatique
- N°3 : Environnement économique
- N°4 : Changements règlementaires
- N°5 : Evènements naturels exceptionnels

Augmentation constante des cyberattaques (extorsion d'agent principalement)

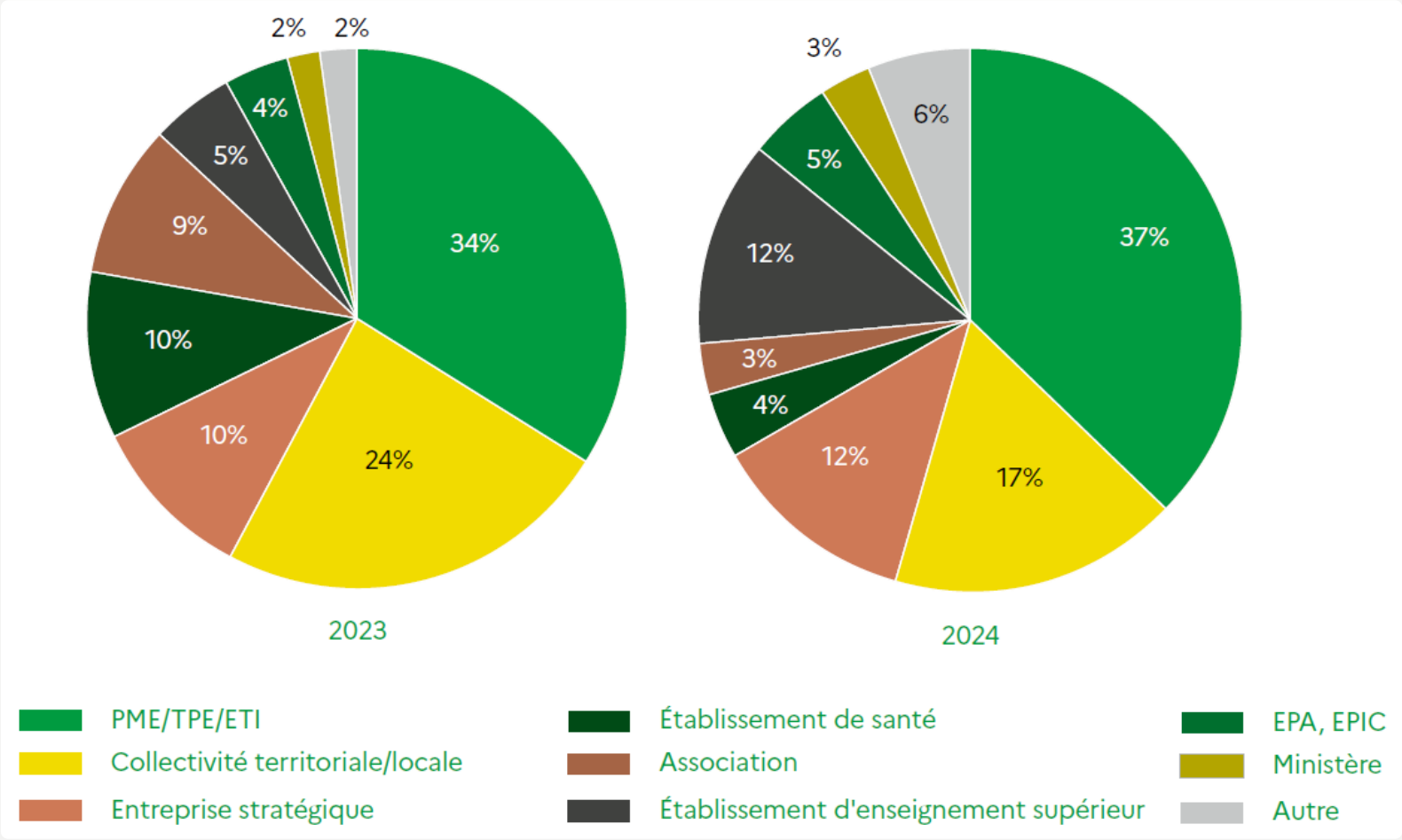
Tensions géopolitiques, exemple : hacktivistes pro-russes

Evolution des techniques : ciblage de structures locales, utilisation de l'IA…

Vulnérabilités dues à la multiplication des prestataires : SS2i, éditeurs, plateformes…

CONTEXTE ACTUEL EN FRANCE

Quelques chiffres : attaques par rançongiciel



EN NOUVELLE-AQUITAINE

2023 : 150 incidents traités par le Campus Cyber de Bordeaux

2024 : 277 incidents traités (secteur privé : 164, secteur public : 113)

Nombre d’incidents déclarés (plaintes) **<<<** nombre d’incidents réels

EN DORDOGNE

En 2024 :

- Défiguration de sites internet : entreprises, mairies…
- Faux Ordre de Virement (FOVI) pour une mairie : préjudice de 42000€
- Usurpation d’identité d’une mairie avec ou sans piratage d’adresse email
- Piratage de comptes Facebook : élus, entreprises…
- Rançongiciel dans 2 grosses associations en fin d’année
- …

LE CADRE RÈGLEMENTAIRE

RGPD et NIS 2 : deux textes européens complémentaires

- **Règlement Général sur la protection des Données :** mai 2018 (application)
- **Network and Information Security 2** - Sécurité des réseaux et des systèmes d'information n°2 : octobre 2024 (transposition dans le droit national en cours)

- Ces directives constitueront à terme le socle des **obligations de sécurisation** des systèmes d'information avec 2 visions : **techniques/organisationnelle** et **juridique**
- Elles sanctuarisent **l'obligation de notification** des incidents de sécurité
- La NIS 2 impose des exigences plus strictes pour **améliorer la sécurité et la résilience** des réseaux et systèmes d'information.
- La NIS 2 encourage les organisations à **sensibiliser leurs employés** à l'importance de la sécurité afin de prévenir les incidents

LES DIFFÉRENTS TYPES D'ATTAQUES ET LEURS VECTEURS

ATTAQUES ET VECTEURS

- **Attaques par messagerie** (emails, sms, WhatsApp, réseaux sociaux…) : pièce jointe, lien, transfert de fichiers, faux courrier…
- Attaques via navigateur : **site web malveillant** prétendant par exemple répondre à un problème et poussant à l'installation de logiciels ou d'extensions du navigateur
- **Attaques de mots de passe** : par force brute ou via un mot de passe compromis utilisé à plusieurs endroits ou par perte/vol d'un accès
- **Attaques par exploitation d'une vulnérabilité / faille de sécurité** : appareils et logiciels non mis à jour ou obsolètes
- Attaques d'ingénierie sociale : exploitation des utilisateurs par le biais d'**usurpation(s) d'identité**, le plus souvent par email, sms ou par téléphone

ATTAQUES ET VECTEURS

- **Appareils mobiles :** applications ou usages malveillants
- **Supports amovibles :** clé USB, disque dur externe…
- Périphériques modifiés : souris, clavier, dongle, borne de recharge de téléphone…
- **Réseaux sans fil publics**
- Réseaux sans fil pro : clé wifi trop simple ou communiquée à l'extérieur, point d'accès wifi trop ancien avec protocole vulnérable : WEP, WPA1…
- QR codes
- Personnes (internes ou externes), volontaires ou victimes d'un cybercriminel

LES ATTAQUES LES PLUS RÉPANDUES

L'HAMEÇONNAGE (PHISHING)

- **Vecteurs** : tout logiciel incluant une messagerie, principalement les sms et les emails (pièce jointe ou lien) dont l'objectif est de vous rediriger vers un site web frauduleux ou de communiquer directement avec l'attaquant par email
  - Pour vous injecter un logiciel malveillant
  - Pour voler des données en imitant un site connu
- **Objectifs de l'attaque** :
  - Vol de mot de passe pour piratage de comptes en ligne
  - Fraudes bancaires
  - Vols de données
  - Installation d'un rançongiciel ou d'un chevale de Troie
  - Usurpation d'identité
  - Fausse amende ou fausse convocation gendarmerie/police/justice

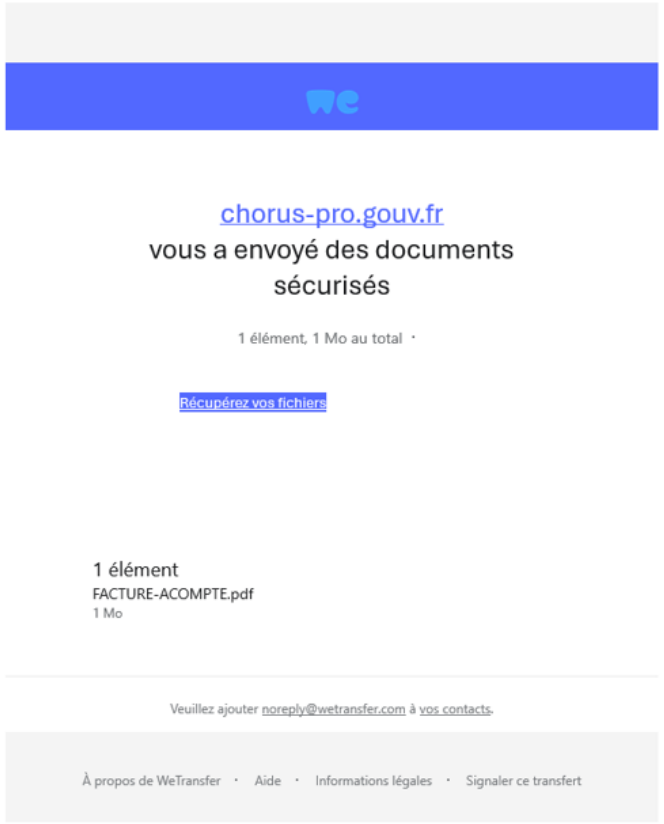
LES RANÇONGICIELS

- **Vecteurs :**
  - Emails, messageries (pièce jointe ou lien)
  - Site web malveillant ou compromis
  - Intrusion dans vos systèmes par l'intermédiaire d'un mot de passe compromis ou d'un logiciel comportant des vulnérabilités non corrigées
- **Objectifs de l'attaque :**
  - 1ère étape : chiffrement silencieux (ou en votre absence) de tous vos dossiers, fichiers, bases de données, emails (stockés sur le poste, sur le réseau local et/ou dans le cloud), les rendant inutilisables
  - 2nde étape : affichage d'un message de demande de rançon à payer en cryptomonnaie

PIRATAGE DE COMPTE

- **Vecteurs :**
  - Les mots de passe (trop simples ou utilisés par ailleurs, récupérés par ruse, par perte, par vol ou par intrusion)
  - L'hameçonnage via messagerie
- **Objectifs de l'attaque :**
  - Vol de vos données personnelles pour usurpation d'identité (nom, prénom, email, adresse postale, téléphone, date de naissance, cordonnées bancaires…)
  - Achats en ligne si votre carte bancaire est sauvegardée dans le compte
  - Récupération de votre mot passe en plus de votre email (mot de passe qui sera donc testé sur d'autres grandes plateformes si le même mot de passe était utilisé sur plusieurs comptes)
  - Message à tous vos contacts alléguant un problème nécessitant l'envoi de fonds à l'étranger

EXEMPLE DE PHISHINGS



chorus-pro.gouv.fr
vous a envoyé des documents sécurisés

1 élément, 1 Mo au total ·

Récupérez vos fichiers

1 élément
FACTURE-ACOMPTE.pdf
1 Mo

Veuillez ajouter noreply@wetransfer.com à vos contacts.

À propos de WeTransfer · Aide · Informations légales · Signaler ce transfert

De : - MAIRIE
Envoyé : mardi 17 septembre 2024 07:50
À : contacts.entreprises@orange.fr
Objet : Facture

Bonjour

Nous vous adressons notre facture / devis N°D2023224, dûment signée, en pièce jointe.
Si cela vous convient, nous vous prions de bien vouloir nous le renvoyer signé et approuvé.

Les fichiers seront expirés dans 2 jours. Après avoir ouvert le dossier, cliquez sur le bouton récupérer les fichiers.

Récupérer les fichiers.

Je vous souhaite une réception sans problème de ces éléments.

Cordialement

Virginie RICHARD
130 RUE DE SAINT-PRIX 95150
06.20.83.03.38

LES FAUX ORDRES DE VIREMENT (FOVI)

- **Vecteurs :**
  - Email, sms
  - Appels téléphoniques
- **Objectifs de l'attaque**
  - Vous faire valider un paiement/virement bancaire frauduleux suite à un prétendu piratage de votre compte bancaire ou carte de paiement
  - Modification d'un RIB fournisseur via une usurpation d'identité

EXEMPLE DE TENTATIVE DE FOVI

M Mairie de Boulazac Isle Manoire <secretariatfournisseurs@gmail.com>

IBAN MAIRIE DE BOULAZAC.... 39 Ko

Chèr(e) Client(e)

Nous vous informons par la présente de la mise à jour de nos coordonnées bancaires .

En effet, nous avons changé de compte bancaire depuis le 20 Novembre 2023.

Nous vous prions de bien vouloir trouver ci-joint notre nouveau RIB (IBAN) pour le règlement de vos prochaines factures.

Merci de bien vouloir nous confirmer par retour de mail la bonne réception des nouvelles coordonnées bancaires.

Vous en souhaitant bonne réception.

Bien cordialement

VILLE DE BOULAZAC Isle Manoire

Mairie de Boulazac Isle Manoire
Espace Agora, Av. de l'Agora,
24750 Boulazac Isle Manoire,
France

BANQUE PALATINE

Destiné à être remis, à leur demande, à vos créanciers ou débiteurs, appelés à enregistrer des opérations sur votre compte (virements, prélèvements, etc.)

RELEVÉ D'IDENTITÉ BANCAIRE

TITULAIRE DU COMPTE

Mairie de Boulazac Isle Manoire
Espace Agora, Av. de l'Agora,
24750 Boulazac Isle Manoire,
France

IDENTIFICATION INTERNATIONAL/SWIFT

CODE IBAN FR76 3000 4031 6800 0030 7786 496

CODE SWIFT/BIC BNPAFRPPXXX

DOMICILIATION BANCAIRE

Banque Palatine

147 Bd Saint-Germain 6ème
75006 Paris
France

FAUX MESSAGES « GENDARMERIE, POLICE, JUSTICE »

- **Vecteurs :**
  - Emails, SMS et tout type de messagerie
- **Objectifs de l'attaque :**
  - Faire payer une « amende en ligne »
  - Chantage (piratage webcam, pédopornographie…)

EXEMPLE : « EMAIL GENDARMERIE »

De : L'Europe Brigade Nationale <cirparis.gendarmerieminister@gmail.com>
Envoyé : mardi 7 décembre 2021 12:37
À : gendarmerieparis@gouv.fr <gendarmerieparis@gouv.fr>
Objet : Rappel: DOSSIER N°322441

DIRECTION GÉNÉRALE DE LA GENDARMERIE

DIRECTION DE PROTECTION DES MINEURES

A votre attention :

CONVOCATION EN JUSTICE

Pour les nécessités d'une enquête judiciaire
(Article 390-1 du Code de procédure pénale)

Je suis M. Christian RODRIGUEZ, directeur général de la gendarmerie nationale en collaboration avec L'Office Européen De Police (Europol). Je vous contacte peu après une saisie informatique de cyber-infiltration (Autorisée, notamment en matière de pédopornographie, Site Pornographique, Cyber pornographie, pour vous informer que vous avez fait l'objet de plusieurs poursuites judiciaires en vigueur :

* LA PÉDOPORNOGRAPHIE
* SITE PORNOGRAPHIQUE
* CYBERPORNOGRAPHIE
* DÉTOURNEMENT DE MINEURS

Vous êtes prié de faire entendre par mail en nous écrivant vos justifications afin qu'elles soient mises en examen et vérifiées de sorte à évaluer les sanctions ; cela dans un délai strict de 72 heures. Passé ce délai, nous nous verrons dans l'obligation de transmettre notre rapport à Mme Maryvonne CAILLIBOTTE, procureur adjoint de la République près le tribunal de grande instance de Versailles et spécialiste de cybercriminalité pour établir un mandat d'arrêt à votre encontre, et vous serez fiché comme délinquant sexuel.

Votre dossier sera également transmis aux médias pour une diffusion où votre famille, vos proches et toute l'Europe entière verront ce que vous avez fait devant votre ordinateur.
Maintenant vous êtes averti.
Cordialement,

Glé. Christian RODRIGUEZ,
directeur général de la gendarmerie nationale.

DIRECTION CENTRALE DE LA GENDARMERIE
BRIGADE DE PROTECTION DES MINEURS
Adresse : 4 rue Claude-Bernard 92130 Issy-les-Moulineaux

LES ARNAQUES AU FAUX SUPPORT TECHNIQUE

- **Vecteurs :**
  - Site web malveillant ou piraté
  - Notification de navigateur ou de téléphone
  - Emails, SMS, chat
  - Appel téléphonique
  - Tout message demandant de contacter un prétendu support technique
- **Objectifs de l'attaque :**
  - Vous faire appeler par téléphone un faux support technique (Microsoft, Google, Amazon…) qui va essayer de vous convaincre d'installer un logiciel malveillant, de payer un pseudo-dépannage ou de vous faire acheter des logiciels inutiles voire nuisibles.

LES PROGRAMMES MALVEILLANTS

- **Un mécanisme de propagation :**
  - **Virus** : dépend souvent d'une action de l'utilisateur (pièce jointe, insertion d'une clé USB, réponse à une demande d'autorisation du logiciel ou du système…)
  - **Ver** : exploite des vulnérabilités sans action de l'utilisateur et peut se répliquer par ailleurs
  - **Cheval de Troie** (Trojan) : se présentant comme un logiciel authentique pouvant même être fonctionnel tout en effectuant des actions malveillantes de manière cachée, telles que le vol d'informations
- **Une « charge utile » (payload) :**
  - Rançongiciel
  - Logiciel espion
  - Porte dérobée
  - Botnet

LES ATTAQUES LOCALES

LES SUPPORTS PHYSIQUES

- **Vecteurs :**
  - Clés USB, disques durs externes
  - Supports optiques (CD, DVD)
  - Potentiellement tout appareil connecté à un poste via USB (appareil mobile, souris, dongle, keylogger…)
  - Borne de recharge de téléphone
- **Objectifs de l'attaque :**
  - Injection d'un logiciel malveillant
    - Virus, malware
    - Rootkit / cheval de Troie / keylogger
    - Rançongiciel
  - Vols de données ou de mots de passe

INGÉNIERIE SOCIALE

- **Vecteurs :**
  - Personnes physiques
  - Appels téléphoniques
- **Objectifs de l'attaque :**
  - Soutirer des informations permettant de compromettre la sécurité de vos systèmes d'information :
    - procédures de travail
    - mots de passe / clé wifi
    - noms et fonctions de personnes travaillant dans votre structure
  - Prendre la main sur une machine non verrouillée pour récupérer des informations ou installer un programme ou équipement malveillant

PRÉVENTION ET MESURES D'ATTÉNUATION

SÉCURISER VOTRE CONNEXION

Se renseigner auprès de votre opérateur fibre et/ou votre prestataire informatique :

- Vérifier que votre **box / routeur opérateur fibre** est à jour et non obsolète (s'applique aussi à l'accès wifi de la box)
- Vérifier qu'un **pare-feu** est activé et bloque toutes les connexions entrantes
  Exception : accès distant sécurisé de type VPN avec certificat de chiffrement
- Vérifier que les accès administrateur à votre box / routeur disposent bien d'un mot de passe fort et que le mot de passe par défaut a bien été modifié
- Activer la double authentification pour l'accès à l'espace client de votre opérateur
- Différencier les accès wifi pro et public
- Clé(s) wifi à renouveler régulièrement (20 caractères minimum)

LES BONS REFLEX

- **Ne jamais répondre directement à une sollicitation** d'où qu'elle provienne (email, sms, appel téléphonique, WhatsApp, réseaux sociaux et toute plateforme disposant d'une messagerie…)
  - Ne jamais cliquer sur un lien depuis un email ou un sms non identifié
  - Ne jamais ouvrir de pièce jointe quel que soit le type
  - Ne jamais répondre au message

- **Toujours vérifier l'information par vos moyens habituels,** sans jamais suivre la procédure issue du message ou de l'appelant vous alertant d'un problème :
  - Vous rendre vous-même sur le site/service par vos moyens habituels
    exemple : se connecter sur le site des impôts ou de votre banque depuis un moteur de recherche ou via vos favoris
  - Contacter par téléphone l'administration, la banque, l'établissement, le client
    exemple : se connecter sur votre compte Amazon via votre application mobile

CONNAITRE L'EXISTENCE DU « SPOOFING »

Définition : le spoofing consiste à usurper une identité électronique pour masquer sa propre identité et ainsi commettre des délits sur Internet

- L'adresse d'expéditeur d'un email peut très facilement être remplacée par n'importe quelle adresse

- Dans certains cas un numéro de téléphone peut être usurpé pour un sms ou des appels (vishing)
  exemple : SMS envoyé depuis le même numéro court avec lequel votre banque vous contacte habituellement

APPRENDRE À RECONNAITRE LES FAUX MESSAGES

- **Indices dans un email** : absence de signature professionnelle, de numéro de téléphone ou autre élément de contexte habituel propre aux échanges entre professionnels
- Même si aléatoire, se rappeler que l'envoi en masse de ce type de messages cible les services les plus répandus pour avoir le maximum de chance d'aboutir.
  Exemples :
  - La majorité des Français sont à la CPAM et ont un compte AMELI et une carte vitale
  - Ciblage au volume : établissements bancaires ayant le plus grand nombre de clients en France :
    - Crédit agricole (53M)
    - Banque populaire (36M)
    - BNP (31M)
    - Société générale (30M)
  - Ciblage de profils plus fragiles via la Banque postale (43% des 75 ans et plus ont un compte dans cet établissement)

LES SERVICES LES PLUS CIBLÉS

- Amazon est le plus gros site de vente en ligne
- Chronopost et Colissimo sont les plus gros transporteurs de colis
- Paypal est le plus gros site de paiement en ligne
- Netflix est la plateforme avec le plus grand nombre d'abonnés
- Rappels d'impayés de la part de l'administration fiscale à la rentrée ou à l'automne (période des avis d'imposition et des taxes foncières…)

AUTRES EXEMPLES :

- L'arnaque à la validité du permis de conduire
- Message vocal soi-disant en attente qui renvoyant vers un site malveillant
- « Ping call » : appel en absence de la part d'un numéro inconnu
- Paiement d'infractions en ligne (ANTAI)
- Appel d'un faux conseiller bancaire
- Message d'un ami en difficulté (piratage de compte)
- …

LES MOTS DE PASSE

- **Mot de passe complexe** :
  - Doit être aléatoire et ne doit contenir aucun mot existant
  - 10 à 16 caractères minimum en fonction de la criticité
  - Doit contenir des majuscules, minuscules, chiffres et au moins un caractère spécial
  - Utiliser un moyen mnémotechnique (exemple : initiales d'une phrase + variations avec chiffres et symboles)
- Ne jamais utiliser 2 fois le même mot de passe (un mot de passe par compte, cf piratage de comptes en ligne)
- Ne jamais saisir son mot de passe si l'on n'est pas soi-même à l'origine de la demande de connexion
- Ne jamais saisir son mot de passe sur une machine étrangère ou pour laquelle on ne maitrise pas la sécurité et/ou l'usage
- Être certain que le site utilise une connexion sécurisée (https, petit cadenas…)
- Ne pas s'identifier sur des comptes critiques depuis des points d'accès wifi public
  (à proscrire obligatoirement sans https)
- Un mot de passe est personnel et ne doit jamais être communiqué à un tiers
- Ne pas écrire ses mots de passe en clair dans un fichier ou sur un post-it près de la machine. Préférer l'usage d'un gestionnaire de mot de passe sécurisé comme **KeePass** ou un coffre-fort numérique)

L'AUTHENTIFICATION À FACTEURS MULTIPLES (A2F, DFA, MFA…)

- Réduit considérablement le risque de piratage de compte avec une efficacité de 100% contre les attaques automatisées
- Différentes méthodes à chaque nouvelle connexion (en plus du mot de passe traditionnel) :
  - Clé de sécurité physique (USB)
  - Authentification biométrique (empreinte, iris…)
  - Application d'authentification dédiée sur smartphone
    exemples : Microsoft/Google Authenticator, Authy…
  - Validation d'accès depuis un appareil tiers
  - Code envoyé par SMS

UTILISER UN ANTIVIRUS

- Aucun système n'est désormais à l'abri : Windows, MacOs, Android, IPhone…
- Vérifier que votre antivirus est toujours actif et à jour
  exemple : centre de sécurité de Windows

- Antivirus payant >>> antivirus gratuit
  Recommandations antivirus : ESET NOD32, SentinelOne, Crowdstrike

SE PROTÉGER DES VULNÉRABILITÉS

Toujours maintenir vos logiciels et appareils à jour :

- Systèmes d'exploitation des appareils : ordinateurs, smartphones, périphériques externes (dont webcams)…
- **Mettre à jour vos logiciels** dés que l'on vous le propose : logiciels professionnels, bureautique, sites web (en l'absence de contrat de maintenance incluant les mises à jour de sécurité par votre prestataire web)
  NB : 90% des sites web attaqués dans le monde utilisaient un Wordpress
- Vérifier que les **mises à jour automatiques** sont bien activées sur tous vos appareils et logiciels qui le permettent
- En cas de doute consultez les alertes de sécurité en cours sur le site **cert.ssi.gouv.fr**

SE RENSEIGNER SUR D'ÉVENTUELLES COMPROMISSIONS DE VOS COMPTES

Il est possible qu'un prestataire ou un service où vous avez créé un compte ait été victime d'un piratage. Une base de données mondiale régulièrement mise à jour recense toutes les données piratées qui ont déjà été divulguées publiquement :

- Se rendre sur le site web **haveibeenpwned.com**
- Saisir votre adresse email dans le champ « email address »
- Si l'on vous indique que votre adresse email a été compromise suite à un précédent piratage (par exemple le piratage de l'éditeur du pdf Adobe en 2013), le site vous indiquera quel(s) type(s) de données ont été récupérées par les pirates
- S'il est indiqué que le mot de passe (password) fait parti des données usurpées, il est nécessaire de le modifier en urgence à tous les endroits où il aurait été utilisé

AMÉLIORER SON « HYGIÈNE NUMÉRIQUE »

- Ne pas stocker les mots de passe en clair dans les machines
  Exemples : fichiers bloc-notes ou Excel avec une liste de mots de passe
- Ne pas noter les mots de passe sur des notes papier accessibles (post-it, documents papier dans une sacoche d'ordinateur portable etc.). Privilégier l'utilisation de coffres forts numérique ou de gestionnaires de mots de passe
  Exemple : logiciel libre gratuit ***Keepass***
- Eviter de transmettre des identifiants et mots de passe en clair par email ou tout autre système messagerie (sms, chat, messageries de réseaux sociaux…)
  Le cas échéant modifier immédiatement le mot de passe transmis de manière non sécurisée
- Activer le verrouillage automatique du poste après inactivité
- Toujours éteindre son poste le soir ou avant une absence
- Toujours se déconnecter d'un bureau à distance

SE PROTÉGER, PRÉVENIR ET AGIR

En entreprise : augmenter la sécurité de sa structure

- Se renseigner sur la présence d'un **pare-feu**, sur sa configuration, son suivi et ses mises à jour
- Investir dans des solutions de sécurité avancées managées (MDR) :
  - **EDR** : solutions de détection et de réponse conçues pour surveiller et détecter les activités malveillantes (ou sortant des habitudes d'utilisation) directement sur les postes des utilisateurs afin d'y répondre manuellement (alertes) et automatiquement
  - **XDR** : solutions de détection étendues agrégeant plusieurs sources de détection (postes, réseaux, cloud) en corrélant des données de différentes sources et reposant sur un apprentissage automatique
  - **SOC** : équipe de veille (le plus souvent externalisée) dédiée à la surveillance et à la réponse en temps réel des alertes de sécurité (pouvant provenir des EDR/XDR)

SOUSCRIRE UNE ASSURANCE CYBER

Réduire les couts et impacts en cas de sinistre

- Prime annuelle entre 500€ et 1500€ (en fonction du budget, des effectifs, de la couverture et de la franchise choisie)
- Permet de couvrir les frais d'analyse forensique (investigation sur la source de l'attaque), de remise en service et de perte de recettes
- Permet de couvrir la cyberfraude (faux ordres de virements, usurpations d'identité…)
- Préférer une compagnie d'assurance spécialisée en Cybersécurité avec un service dédié à l'accompagnement en cas de sinistre
  exemples : Stoïk (recommandé pour leur prévention active), Onlynnov, Dattak…

PRÉVENTION ET MESURES D'ATTÉNUATION:

LES SAUVEGARDES

LES SAUVEGARDES PHYSIQUES

Stockage sur plusieurs appareils, disque dur externe, clé USB, carte SD, support optique…

- Vos données doivent être stockées à minima sur **2 supports différents** et **vérifiées régulièrement**
- Aucun stockage physique n'est infaillible et la plupart ont des durées de vie limitées :
  - Disque dur : 5 à 7 ans en moyenne (peut être réduit à 3 ans en cas d'usage intensif)
  - Clé USB : entre 10 et 30 ans pour du matériel de marque haut de gamme, beaucoup moins pour du low cost
- **Sécuriser l'accès aux sauvegardes** physiques pour les protéger contre les accès non autorisés et contre le vol
- Essayer d'éloigner les sauvegardes des originaux afin de les protéger d'un dégât naturel ou d'un incendie par exemple
- Préférer les sauvegardes automatiques « descendantes » aux sauvegardes « remontantes » : sauvegardes initiées par le système de sauvegarde externe qui vient récupérer les données dans le stockage plutôt que le contraire. Il est bien sûr utile de vérifier que le système de sauvegarde externe est à jour et ne comporte pas de vulnérabilités connues
- En cas de souscription d'un contrat d'assurance sur la perte de données, bien vérifier les clauses et obligations du contrat

LES SAUVEGARDES ET DONNÉES CLOUD

- Vérifier que 100% de vos données importantes sont bien dans le cloud ou sauvegardées dans le cloud (dossiers locaux documents/scan, bureau du système d'exploitation, données d'applications locales ou de logiciels de gestion…)

- Certains services cloud ne proposent par défaut que des sauvegardes de fiabilité de service (contre les pannes de leur infrastructure). Ce type de sauvegarde ne permet pas de récupérer vos données suites à une attaque de type rançongiciel ou d'effacement malveillant (mais aussi contre les erreurs humaines).
  Exemple : Microsoft 365 nécessite le déploiement d'une solution de sauvegarde tierce de vos données (emails, documents bureautique, agendas…) ou la souscription d'un service supplémentaire : Microsoft 365 backup

- Vérifier que les sauvegardes cloud répondent bien aux exigences du RGPD (sécurisation/chiffrement des données, localisation dans l'UE…)

LES SAUVEGARDES ET DONNÉES CLOUD

- Se renseigner sur la politique de sauvegarde votre prestataire cloud :
  - **Fréquence des sauvegardes** : temps réel, biquotidienne, quotidienne, hebdomadaire
  - **Durée de rétention** de chaque sauvegarde : 1 semaine, 3 semaines, 3/6 mois…
    A mettre en corrélation avec les plus longues périodes d'absence ou de fermeture possibles.
  - Type d'options incluses ou pas :
    - **Versioning** : conserver plusieurs versions dans le temps
    - **Granularité** : possibilité de récupérer uniquement certains fichiers et/ou à certaines dates en combinant avec le versioning
  - Être attentifs aux éventuelles limitations de l'offre, comme par exemple un volume de données maximum qui pourrait ne pas être suffisant pour la durée de rétention souhaitée

PRÉVENTION ET MESURES D'ATTÉNUATION:

10 BONNES PRATIQUES

1. Utiliser des **mots de passe forts et différents** pour chaque service
   (*moyen mnémotechnique : phrase clé avec préfixes et suffixes variables)*
2. Toujours effectuer les **mises à jour de sécurité** sur vos équipements
3. Ne jamais ouvrir les **pièces jointes** et ne jamais cliquer sur des **liens** provenant de message dont vous n'êtes pas certain de connaître l'expéditeur
4. Installer et maintenir à jour un **antivirus** et **un pare-feu**
5. Faire des **sauvegardes régulières vérifiées** en conservant toujours une sauvegarde hors ligne
6. Toujours séparer **usages personnels** et **professionnels**
7. Toujours télécharger vos applications depuis des **sites officiels** et ne jamais installer d'application dont on n'est pas certain de la probité
8. Eviter d'utiliser des comptes avec des **droits administrateur**
9. Utiliser dés que possible des **authentifications à double facteur**
10. Ne pas laisser vos équipements sans surveillance ou sans protection d'accès

QUE FAIRE EN CAS DE CYBERATTAQUE

EN URGENCE

- **Déconnecter la machine attaquée** du réseau local et d'internet (débrancher le câble réseau, couper la connexion wifi et/ou désactiver une connexion de type partage de données depuis un appareil mobile). Cette mesure permet de stopper et d'éventuellement limiter la propagation de l'attaque à d'autres machines et données.
- Ne pas éteindre la machine afin de permettre à un expert d'analyser l'attaque plus tard *(sauf dans le cas d'une attaque qui vient de débuter et/ou incontrôlable)*
- Alerter au plus vite **votre support informatique** pour leur demander d'intervenir en urgence
- **Ne plus utiliser l'équipement** compromis tant que la situation n'a pas été résolue
- **Prévenir vos collègues** de l'attaque en cours
- En cas de suspicion de fraudes bancaires, contacter votre agence
- **Sauvegarder toutes les données de votre entreprise** et les logiciels installés sur votre système d'information

DANS UN SECOND TEMPS

- Essayer d'évaluer les préjudices : données et service impactés
- Si vous avez souscrit un contrat, contacter votre assurance perte de données
- Essayer d'identifier la faille qui a permis la cyberattaque et mettre à jour le logiciel ou le système vulnérable
- Demander un diagnostic personnalisé en ligne sur **cybermalveillance.gouv.fr**
- En cas de rançongiciel, ne jamais payer la rançon demandée
- Vérifier l'intégrité de vos sauvegardes afin de planifier une reprise d'activité
- En cas de violation de données personnelles, vous devez effectuer en ligne une notification auprès de la CNIL dans les 72h (RGPD et NIS2)
- Porter plainte (avec pré-plainte en ligne)
- Vous pouvez aussi demander de l'aide auprès du Centre de Ressources Cybersécurité de la Dordogne (CRC 24)

POUR ALLER PLUS LOIN

WEBOGRAPHIE

Retrouvez les supports, liens utiles, RGPD, sites d'information, webinaires du CRC24 et bien plus encore sur

cyber.assoligue.org

MERCI DE VOTRE ATTENTION