Atelier de sensibilisation aux risques Cyber

21 janvier 2025

Proxim CYBERSOLUTIONS

UIMM Yonne – LA FABRIQUE DE L'AVENIR

Yonne

Sommaire

1. Introduction (10 min)
2. Contexte et enjeux de la cybersécurité en TPE/PME (15 min)
3. Panorama des cybermenaces actuelles (20 min)
4. Les bases d'une bonne hygiène numérique (20 min)
5. Réglementation et obligations légales (15 min)
6. Atelier pratique : reconnaître les signaux d'une attaque (25 min)
7. Ressources et outils utiles (10 min)
8. Questions / réponses et conclusion (5 min)

Introduction

Introduction

- Objectifs :
  - Vous sensibiliser
  - Comprendre les risques cyber
  - Adopter des bonnes pratiques

01 Liste des entreprises victimes d'une cyberattaque en 2024-2025

(liste évidemment non exhaustive…)

- Viamedis - 1 février 2024 - Fuite massive de données d'assurés
- Almerys - 1 février 2024 - Fuite massive de données d'assurés
- Etesia - 2 février 2024 - Ransonware
- Sidaction - 28 février 2024 - Vol de données des donateurs
- Hoya et Seiko - 29 mars 2024 - Intrusion dans un serveur et interruption partiel de la production
- Paris Saint-Germain Football Club (PSG) - 3 avril 2024 - Tentative d'intrusion sur la billetterie
- Le Slip Français - 15 avril 2024 - Vol de données de 696 000 clients
- Speedy France - 19 avril 2024 - Vol de données personnelles
- Dropbox Sign - 24 avril 2024 - Fuite de données personnelles et d'authentification
- Dell - 28 avril 2024 - Fuite de données clients et revente sur le dark web
- Axido - 14 juin 2024 - Ransomware
- SCAM (Société civile des auteurs multimédia) - 21 juin 2024 - Ransomware
- Synertrade - 27 juin 2024 - Vol de données par le groupe de Ransomware Cactus
- Forum Sirius - 28 juin 2024 - Vol de données affectant 400 salles de spectacles en France
- Pharmacie Orléans à Saumur - 30 juin 2024 - Fuite de données de 50 000 patients
- Lagoon - 17 août 2024 - Rançongiciel et interruption d'internet pour des milliers de Néo-calédoniens

01 Liste des entreprises victimes d'une cyberattaque en 2024-2025

(liste évidemment non exhaustive…)

- Octave.biz - 19 août 2024 - Ransomware
- Antenne Réunion et autres radios de l'Océan Indien - 21 août 2024 - Interruption de la diffusion des programmes
- Cultura - 6 septembre 2024 - Fuite de données personnelles de 1,5 million de clients
- La Croix (Groupe Bayard) - 8 septembre 2024 - Rançongiciel paralysant outils rédactionnels et commerciaux
- Meilleurtaux - 27 septembre 2024 - Fuite de données sensibles incluant les revenus et la situation professionnelle des clients
- Free - 22 octobre 2024 - Fuite de données de 19 millions d'abonnés et 5 millions d'IBAN via accès interne compromis
- Auchan - 19 novembre 2024 - Fuite de données personnelles de 500 000 clients
- Direct Assurance - 20 novembre 2024 - Fuite de données de 6 137 clients et 9 517 prospects
- 8 banques françaises - 6 décembre 2024 - Malware Android DroidBot ciblant les identifiants bancaires des clients (Boursorama, BNP Paribas, Crédit Agricole, Caisse d'Épargne, etc.
- Ecritel - 8 décembre 2024 - Tentative d'intrusion, vol partiel de données internes (270 Go revendiqués)
- Top Achat - 14 décembre 2024 - Fuite de données personnelles non exploitées

01 Liste des organisations publiques victimes d'une cyberattaque en 2024
(liste évidemment non exhaustive…)

- Conseil départemental de la Sarthe - 24 janvier 2024 - Tentative d'intrusion ratée
- Lycées d'Ile-de-France - 20 mars 2024 - Piratage de l'ENT et envoi de menaces d'attentat, revendiqué par l'État Islamique
- Villes de Saint-Nazaire, Pornichet, Montoir-de-Bretagne, Donges et La Chapelle-des-Marais - 9 avril 2024 - Ransomware
- Mairie d'Albi - 22 avril 2024 - Malware
- Ville de Gravelines - 25 avril 2024 - Cryptovirus
- Gouvernement de la Nouvelle-Calédonie - 22 mai 2024 - Attaque par déni de service (DDoS)
- Mairie de Fleury-les-Aubrais - 24 juin 2024 - Ransomware
- Département de la Loire-Atlantique - 16 juillet 2024 - Tentative d'intrusion des réseaux
- Région Pays de la Loire - 19 juillet 2024 - Ransomware par le groupe de hackers Lockbit
- Ville de Reims - 3 septembre 2024 - Attaque par déni de service (DDoS) par un groupe pro-russe
- La Réunion - 14 novembre 2024 - Ransomware avec fuite limitée de données administratives

01 Liste des organisations publiques victimes d'une cyberattaque en 2024
(liste évidemment non exhaustive…)

- Hôpitaux et établissements de santé
  - CHU de Nantes - 14 janvier 2024 - Attaque par déni de service (DDoS)
  - Ehpad Saint-Jean-Baptiste de Farébersviller - 2 février 2024 - Rançongiciel
  - Centre hospitalier d'Armentières - 11 février 2024 - Demande de rançon
  - Hôpital Simone-Veil à Cannes - 16 avril 2024 - Ransomware revendiqué le groupe de hackers Lockbit et publication de 61 gigaoctets de données confidentielles
  - Groupe d'imagerie médicale Coradix-Magnescan - 3 mai 2024 - Tentative d'intrusion mais aucun vol de données
  - Hospi Grand Ouest - 3 octobre 2024 - Attaque ciblant une clinique, perturbation des services
- Ministères
  - 800 services de l'État français en ligne - 10 mars 2024 - Attaque par déni de service (DDoS)
  - Prestataire du ministère du Travail - 24 octobre 2024 - Fuite de données personnelles de jeunes accompagnés par les Missions locales
- Autres
  - Caisse d'Allocations Familiales (CAF) - 12 février 2024 - Vol des données de 600 000 allocataires à l'aide d'identifiants obtenus illégalement, attaque revendiquée par le groupe de hackers LulzSec
  - France Travail (ex-Pôle emploi) - 13 mars 2024 - Fuite des données de 43 millions de demandeurs d'emploi français
  - Fédération Française de Football (FFF) - 21 mars 2024 - Fuite de données de grande ampleur
  - CCI Pau Béarn - 13 mai 2024 - Ransomware
  - Boutiques de 40 musées français dont le Grand Palais et le Louvres - 3 août 2024 - Ransomware
  - Université Paris-Saclay - 11 août 2024 - Ransomware
  - Caisse d'Allocations Familiales (CAF) - 22 août 2024 - Mise en vente des données de 60 000 allocataires sur le DarkWeb
  - Université Paris-1 Panthéon-Sorbonne - 10 octobre 2024 - Extraction de données de 73 000 étudiants et enseignants
  - Chambre d'Agriculture de Lozère - 20 novembre 2024 - Piratage perturbant les systèmes internes

Et plus localement ?

- Ville de Chalon-sur-Saône – 2021 – 500 k€
- INRAE – décembre 2023
- La communauté de communes de Nuits-Saint-Georges – 15 mars 2024
- Août 2024 : DIVIA Mobilités (Dijon) – vol de données

Contexte et enjeux de la cybersécurité en TPE/PME

- Les TPE/PME sont des cibles privilégiées :
  - Faible budget dédié
  - Absence d'équipe IT spécialisée

- Impact des attaques :
  - Perte de données clients
  - Dégradation de la réputation
  - Coût financier élevé

1. Des TPE-PME conscientes des risques cyber

Pour ces catégories d'entreprises et notamment les plus petites structures,

- la gestion de l'informatique est du ressort du chef d'entreprise (82%);
- 72% ne disposent d'aucun salarié dédié à cette tâche
- budget en sécurité informatique est de moins de 2 000€ par an pour 68% d'entre-elles.
- Dans 53% de ces entreprises les salariés utilisent des moyens personnels à des fins professionnelles dont
  - pour 95% leur téléphone portable,
  - 34% leur ordinateur et
  - 28% leur messagerie personnelle.

1. Des TPE-PME conscientes des risques cyber

Quand on les interroge sur le sujet de la cybersécurité:

- **6 entreprises sur 10 (58%) considèrent que c'est un sujet qui doit mobiliser tout le monde**.
- plus de la moitié (55%) d'entre elles sensibilisent leurs collaborateurs,
- davantage encore dans les grandes entreprises
  - 79% des entreprises de 50 salariés et
  - plus et 71% des entreprises de 10 à 49 salariés.

1. Des TPE-PME conscientes des risques cyber

Parmi les obstacles invoqués pour atteindre le bon niveau de cybersécurité , la moitié (46 %) invoque :

- le manque de temps (60%),
- le manque de connaissances / expertise (56%),
- le manque de budget (53%)
- ou encore ne pas savoir pas vers qui se tourner (34%).

1. Des TPE-PME conscientes des risques cyber

Et 6 entreprises sur 10 (61%) **déclarent être faiblement protégées** (42%) notamment parmi celles de plus de 10 salariés ou **ne pas savoir l'évaluer** (19%).

En matière de sécurité informatique, pour s'informer ou se faire aider, les entreprises se tournent prioritairement vers leur prestataire informatique, notamment celles qui ont une gestion externalisée totale ou partielle (80%). En deuxième position, 1 sur 5 a recours à Cybermalveillance.gouv.fr, et ce davantage encore dans les plus grandes entreprises (51% des entreprises de 50 salariés et plus).

2. Des TPE-PME qui en sous-estiment les enjeux

Malgré cette « prise de conscience » face à la menace cyber, **62% des entreprises interrogées pensent être faiblement exposées aux risques de cyberattaques** (41%) **ou l'ignorent** (21%).

Seules 38% sont conscientes d'être fortement exposées aux risques de cyberattaques.

La plupart **78% se disent insuffisamment préparées** (46%) ou **l'ignorent** (32%) et 7 entreprises sur 10 ne disposent pas de procédure de réaction.

En matière d'équipements, si près de 7 entreprises sur 10 déclarent connaître des solutions de sécurité, plus d'1 sur 2 (53%) **ne sait pas si ces solutions sont adaptées ou non à ses besoins** (42%) **ou pense qu'elles ne le sont pas** (11%).

Enfin, en termes de budget, seules 10% **prévoient de l'augmenter**, notamment celles de plus de 10 et 50 salariés, principalement pour faire évoluer leurs équipements.

3. Des TPE-PME qui témoignent d'un défaut de compétence et d'expertise en cyber

Enfin, quand on leur demande de se projeter dans une situation de cyberattaque, les entreprises reconnaissent que si elles y étaient confrontées, **65% ne sauraient pas en évaluer les impacts ; seules 35% d'entre elles pensent qu'elles seraient en capacité de le faire**, et particulièrement celles qui sont conscientes d'avoir un faible niveau de protection.

Ces mêmes **TPE-PME redoutent un certain nombre d'impacts liés à la cybersécurité** : plus de 9 entreprises sur 10 craignent une destruction ou vol de données (94%), une perte financière (94%) et une interruption d'activité (90%) voire une atteinte à la réputation (80%).

15 % des entreprises interrogées déclarent avoir été touchées par un incident de cybersécurité durant les 12 derniers mois. Ces incidents seraient liés :

- à un hameçonnage (24%),
- au téléchargement d'un virus (18%),
- ou encore à une faille de sécurité non corrigée pour 14% d'entre elles.

3. Des TPE-PME qui témoignent d'un défaut de compétence et d'expertise en cyber

Toutefois, près d'une sur 2 (43%) ne sait pas en expliquer les raisons.

En corrélation avec les risques redoutés évoqués ci-dessus, les principaux impacts pour les entreprises touchées sont :

- l'interruption d'activité (35%),
- le vol de données (25%),
- l'atteinte à l'image de l'entreprise (17%),
- la perte financière (15%),
- la destruction de données (12%).

Panorama des cybermenaces actuelles

Panorama des cybermenaces actuelles

- Phishing :
  - Emails frauduleux pour voler des informations
- Ransomware :
  - Chiffrement des données avec demande de rançon
- Erreurs humaines :
  - Clics sur des liens douteux, mots de passe faibles
  - Plus fort vecteur de cyberattaque, > 70% …

- ----- Dans une moindre mesure ----------
- Intrusions :
  - Via une faille de sécurité ou un accès compromis
  - Mot de passe wifi obsolète, IoT peu sécurisé, switch ou routeur dont le mot de passe n'a jamais été changé (admin/admin)

Les bases d’une bonne hygiène numérique

- Pratiques recommandées :
  - Mots de passe robustes et uniques, jamais communiqués
  - Authentification multifactorielle (MFA)
  - Sauvegardes régulières : le 3-2-1
    - Vous créez trois copies de vos données : les données d'origine sur votre appareil principal et au moins deux copies.
    - Vous utilisez deux périphériques de stockage différents - ici, c'est à vous de choisir les deux supports de stockage - votre PC, un disque dur externe, une clé USB, un DVD, un NAS ou des périphériques de stockage en nuage.
    - Vous conservez l'une des copies de sauvegarde hors site : en conservant des copies de vos données dans un emplacement distant, vous évitez la perte de données due à un sinistre local ou à un scénario de défaillance spécifique au site.

Top 10 des mots de passe en 2024
No comment ...

1. 123456
2. 123456789
3. azerty
4. qwerty123
5. qwerty1
6. azertyuiop
7. marseille
8. doudou
9. loulou
10. 12345678

COMBIEN DE TEMPS FAUT-IL À UN PIRATE POUR TROUVER VOTRE MOT DE PASSE 2024

12 x RTX 4090 | bcrypt

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minescules	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	3Bd ans
17	1k ans	13Md ans	1Bd ans	35Bd ans	276Bd ans
18	11k ans	350Md ans	91Bd ans	2Tn ans	19Tn ans

HIVE SYSTEMS

› www.hivesystems.com/password

ATTENTION

Site qui veut vous aider, mais ne vous aidera pas :
Vous êtes invités à tester votre mot de passe…
Mais que devient-il ensuite ?….

- https://inforisque.fr/fiches-pratiques/tester-mot-de-passe.php

Comment créer un mot de passe fort ?

Lorsque vous réfléchissez à de bonnes idées de mots de passe, vous devez garder à l'esprit les critères suivants :

- Longueur du mot de passe
  - Un mot de passe robuste doit être d'une longueur significative, généralement entre 12 et 15 caractères. Plus le mot de passe est long, plus il devient difficile à déchiffrer pour les pirates.
- Combinaison de caractères
  - Pour renforcer la sécurité, votre mot de passe doit intégrer une variété de caractères, y compris des lettres, des chiffres et des caractères spéciaux. Les espaces peuvent également être utilisés pour accroître la complexité.
- Éviter les évidences
  - Il est essentiel d'éviter l'utilisation de mots courants, de noms de produits, de personnages ou de tout autre élément facilement identifiable. Les hackers utilisent des attaques par dictionnaire, et un mot de passe trop évident est une vulnérabilité majeure.

Comment créer un mot de passe fort ?

- Connaissance exclusive
  - Votre mot de passe doit être une combinaison secrète que vous seul connaissez. Évitez les informations facilement accessibles ou devinables par d'autres. Optez pour des éléments personnels ou des associations uniques que vous pouvez facilement mémoriser.
- Unicité des mots de passe
  - Chaque compte en ligne doit avoir un mot de passe unique. Ne pas réutiliser les mots de passe pour plusieurs comptes est crucial. Si un mot de passe est compromis, cela n'affectera pas la sécurité de vos autres comptes. La diversité des mots de passe est une barrière essentielle contre les atteintes à la sécurité en cascade.

10 Règles d'or de la cybersécurité

1. Utilisez des mots de passe robustes.
   - Exemple : Une phrase de passe comme J@imeMonEntreprise2023!
2. Changez régulièrement vos mots de passe.
   - Évitez de réutiliser les mêmes mots de passe pour plusieurs services.
3. Activez l'authentification multifactorielle (MFA).
   - Ajoutez une couche de sécurité avec un code envoyé sur votre téléphone.
4. Sauvegardez vos données régulièrement.
   - Utilisez un disque dur externe **chiffré** ou une solution cloud sécurisée.
5. Mettez à jour vos logiciels et systèmes.
   - Installez les mises à jour dès qu'elles sont disponibles.
6. Ne cliquez pas sur des liens suspects.
   - Vérifiez l'adresse des liens en survolant avant de cliquer.
7. Protégez vos appareils avec un antivirus.
   - Assurez-vous que l'antivirus est actif et à jour.
8. Formez vos collaborateurs à la cybersécurité.
   - Organisez des sessions régulières de sensibilisation.
9. Limitez les accès aux données sensibles.
   - Accordez les droits d'accès uniquement aux personnes qui en ont besoin.
10. Vérifiez les expéditeurs de vos emails.
    - Soyez vigilant aux emails provenant d'expéditeurs inconnus ou suspects.

Réglementation et obligations légales

- RGPD :
  - Règlement Général sur la Protection des Données
  - Obligation de protéger les données personnelles
  - Notification à la CNIL (Commission Nationale de l'Informatique et des Libertés) en cas de violation
- NIS2 (Network & Information Systems v2) :
  - Obligations spécifiques pour les PME critiques

Le RGPD en 6 points

1. Licéité, loyauté et transparence

Les données personnelles doivent être collectées et traitées de manière légale, dans le respect des droits des personnes concernées.

Les entreprises doivent informer clairement les individus sur :

- Les finalités du traitement (à quoi servent leurs données ?).
- Leur droit d'accès, de rectification et d'opposition.

Exemple : Lors de l'inscription à une newsletter, une case à cocher doit permettre d'accepter explicitement l'utilisation des données.

2. Limitation des finalités

Les données personnelles doivent être collectées pour des objectifs spécifiques, explicites et légitimes.

Une fois les finalités atteintes, les données ne peuvent pas être utilisées pour d'autres usages sans consentement.

Exemple : Les coordonnées d'un client recueillies pour une commande ne peuvent pas être utilisées pour envoyer des offres promotionnelles, sauf consentement.

Le RGPD en 6 points

3. Minimisation des données

Les entreprises doivent limiter la collecte des données à ce qui est strictement nécessaire pour atteindre les objectifs déclarés.

Cela limite le stockage et l'exploitation excessive des informations sensibles.

Exemple : Pour une inscription à un service, demander uniquement le nom, prénom et email, et non des données non pertinentes comme l'adresse complète.

4. Sécurité des données

Les entreprises doivent prendre toutes les mesures techniques et organisationnelles nécessaires pour garantir la confidentialité, intégrité et disponibilité des données.

Cela inclut la protection contre les accès non autorisés, les pertes ou les cyberattaques.

Exemple : Mettre en place des mots de passe sécurisés, un chiffrement des bases de données, et des sauvegardes régulières.

Le RGPD en 6 points

5. Droits des personnes concernées

Le RGPD renforce les droits des individus sur leurs données personnelles :

- Droit d'accès : savoir quelles données sont collectées et comment elles sont utilisées.
- Droit à la rectification : corriger des erreurs dans les données.
- Droit à l'effacement (droit à l'oubli) : demander la suppression des données non nécessaires.
- Droit à la portabilité : récupérer ses données dans un format transférable.
- Droit d'opposition : refuser l'utilisation des données, notamment à des fins marketing.

Exemple : Une personne peut demander à une entreprise de supprimer son compte et ses données associées.

Le RGPD en 6 points

6. Notification des violations de données

En cas de fuite ou de violation de données personnelles, les entreprises ont l'obligation :

- D'informer la CNIL dans les 72 heures.
- De notifier les personnes concernées si le risque pour leurs droits est élevé.

Exemple : En cas de cyberattaque compromettant des données clients, l'entreprise doit alerter la CNIL et les clients concernés.

Rôle de la CNIL

La CNIL est l'organisme français chargé de veiller au respect du RGPD. Ses missions incluent :

1. Conseiller et accompagner : Offrir des guides et des outils pour aider les entreprises à se conformer.
2. Contrôler : Mener des audits et inspections pour vérifier la conformité.
3. Sanctionner : Infliger des amendes en cas de manquement. Les sanctions peuvent aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial.
4. Informer les citoyens : Permettre à toute personne de signaler un abus ou de faire valoir ses droits.

Synthèse sur la Directive NIS2

La directive NIS2 (Network and Information Systems 2), adoptée par l'Union européenne en 2022, renforce les exigences en matière de cybersécurité pour les entreprises et les organisations essentielles.

Objectif principal :

Améliorer la résilience et la gestion des incidents dans les secteurs critiques pour réduire les cyberrisques à l'échelle européenne.

Points clés :

1. Champ élargi : La NIS2 s'applique à un plus grand nombre de secteurs et d'entreprises, notamment :
   - Énergie, transports, santé, services financiers, gestion des déchets.
   - Fournisseurs numériques (cloud, data centers, plateformes en ligne).
2. Obligations renforcées :
   - Mise en place de mesures de sécurité : gestion des risques, protection des systèmes, surveillance, sauvegardes.
   - Gestion des incidents : signaler les incidents significatifs aux autorités nationales compétentes.

Synthèse sur la Directive NIS2

3. Responsabilité accrue :

   Les dirigeants des organisations sont tenus responsables de la mise en œuvre des mesures de cybersécurité. Des sanctions financières peuvent être infligées en cas de non-conformité.

4. Harmonisation européenne :

   La directive introduit des standards communs pour tous les États membres afin d'améliorer la coopération transfrontalière en cas de cyberincident.

5. Délai de transposition :

   Les États membres doivent intégrer la directive NIS2 dans leur législation nationale d'ici octobre 2024.

Pourquoi c'est important pour les entreprises ?

- Les entreprises couvertes par NIS2 doivent évaluer leurs pratiques actuelles et investir dans des systèmes robustes pour protéger leurs données et opérations.
- Ignorer ces obligations peut entraîner des sanctions lourdes et des risques opérationnels majeurs.

La NIS2 incarne un pas significatif vers une cybersécurité proactive et collective en Europe.

Atelier pratique : reconnaître les signaux d’une attaque

Objectif principal

- Apprendre à reconnaître les signes d'une tentative d'attaque, notamment les emails de phishing et les faux sites web.
- Savoir réagir face à un contenu suspect pour minimiser les risques.

Exemple de phishing

Sujet : **Notification d'impôt**
De : République Française <lettre-info-fiscale@dgfip.finances.gouv.fr>
Date : 8:11
Pour : pc@eila.univ-paris-diderot.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DIRECTION GENERALE DES FINANCES PUBLIQUES 20/10/2009

Notification d'impôt - Remboursement

Après les derniers calculs annuels de l'exercice de votre activité, nous avons déterminé que vous êtes admissible à recevoir un remboursement d'impôt de € 178,80.

S'il vous plaît soumettre la demande de remboursement d'impôt et nous permettre de 10 jours ouvrables pour le traitement.

Pour accéder au formulaire pour votre remboursement d'impôt, cliquez ici

Un remboursement peut être retardé pour diverses raisons. Par exemple la soumission des dossiers non valides ou inscrivez après la date limite.

Le Conciliateur fiscal adjoint

Philippe BERGER

© Ministère du budget, des comptes publics et de la fonction publique

http://www.capitalhouse.com.mx/.secure/

Exemple de phishing

Exemple de phishing

De : support@fr.gandi.net <support@fr.gandi.net>
Envoyé : mercredi 26 juin 2019 10:53
À : contact@[redacted]
Objet : [GANDI] Non renouvellement

Bonjour,

Nous n'avons pas reçu le paiement sur votre dernière renouvellement du domaine [redacted].

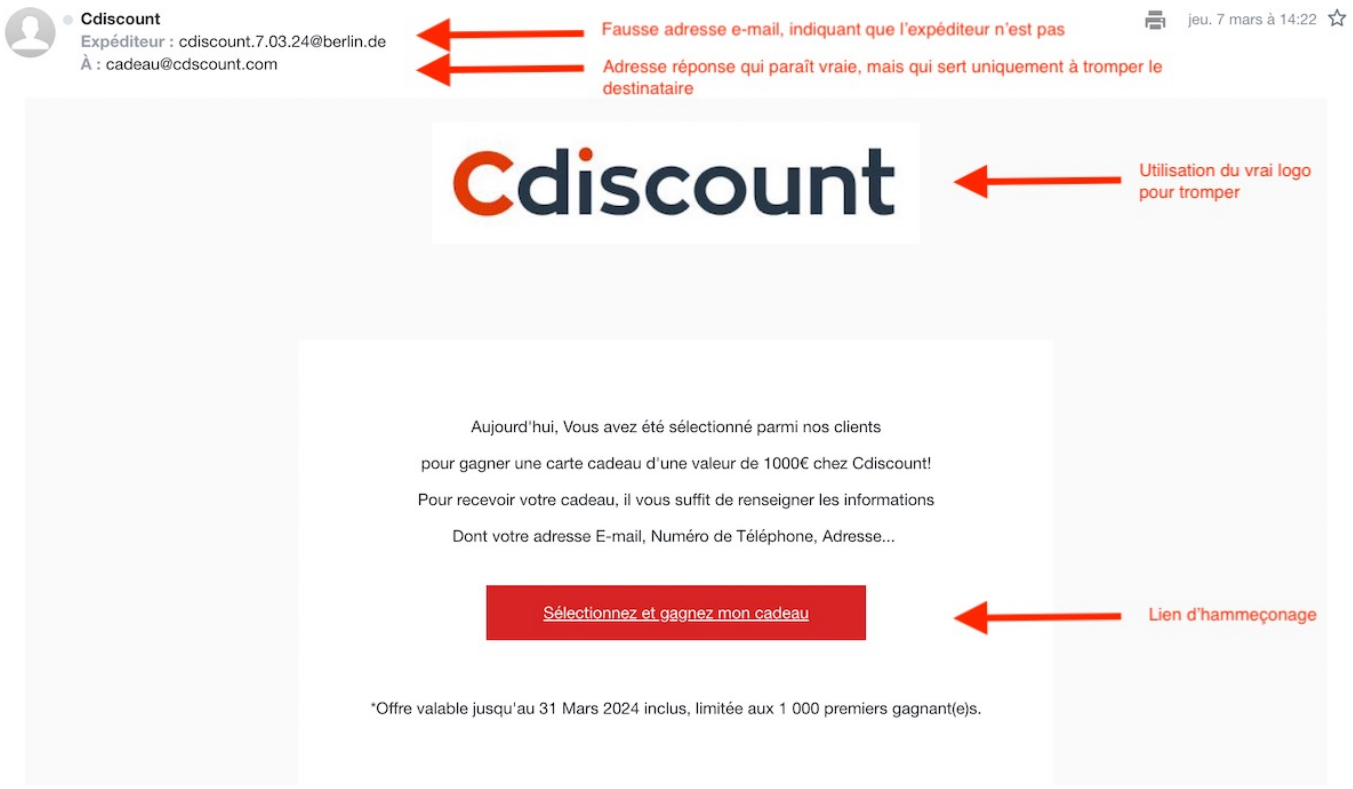
Pour éviter le problème, on vous invite à remplir manuellement le formulaire de renouvellement de vos services suivant les instructions et l[redacted]s:

http://amiljo.se/drive-innov.com
Cliquez pour suivre le lien

Accédez à votre formulaire de paiement.

IMPORTANT : En cas de non règlement sous 48 Heure, votre compte pourrait être définitivement effacé.

Exemple de phishing



Reconnaissance d'un email suspect

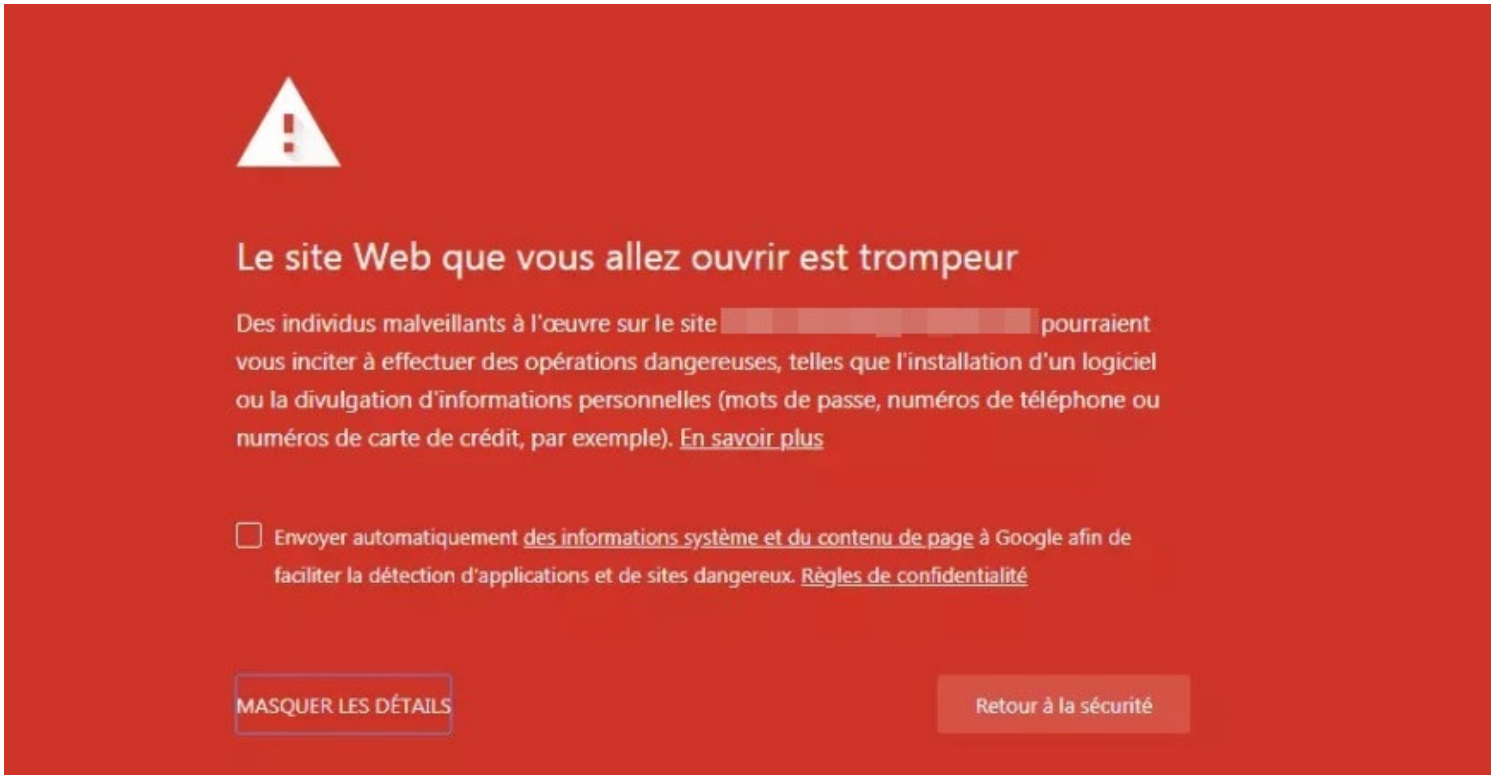
Signes clés à identifier :

- Adresse email frauduleuse (ex. : contact@banqexample.com au lieu de banque.fr).
- Lien suspect ou mal orthographié (ex. : http://banq-login.com).
- Ton alarmiste ou urgent (ex. : « Votre compte sera bloqué dans 24h ! »).
- Erreurs de syntaxe ou de grammaire.

Que faire en cas de doute ?

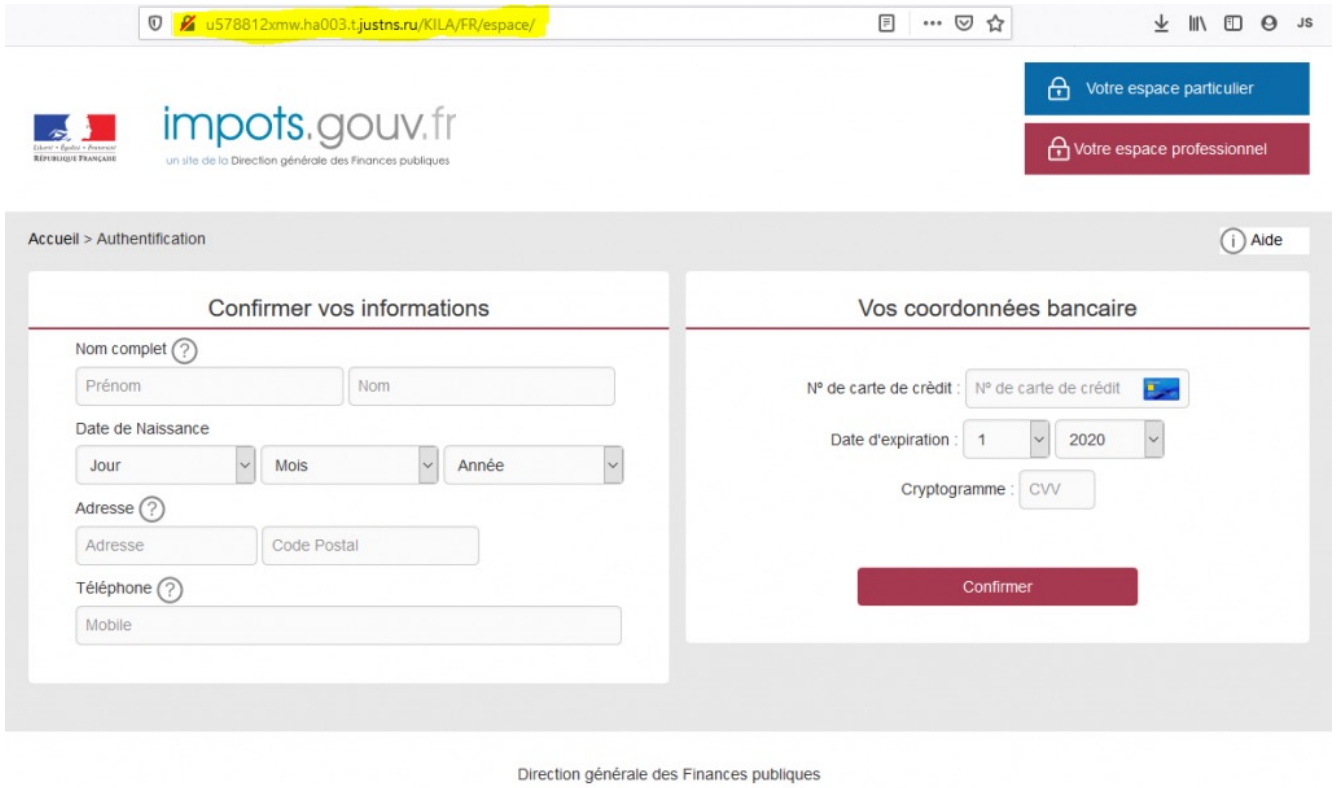
1. Ne pas cliquer sur les liens.
2. Vérifier l'expéditeur.
3. Contacter directement l'entité concernée pour confirmation.

Faux sites web



06 Atelier pratique : reconnaître les signaux d'une attaque

06 Atelier pratique : reconnaître les signaux d'une attaque



Reconnaissance d'un faux site web

Signes clés à identifier :

- URL modifiée ou suspecte.
- Absence de cadenas ou d'indicateurs de sécurité.
- Erreurs dans les textes ou les images.
- Message d'alerte de votre navigateur ou de votre anti-virus

Réponse idéale :

- Signaler immédiatement à l'équipe IT ou à un responsable.
- Déconnecter l'appareil du réseau si une erreur a été commise.
- Lancer une analyse antivirus/malware.

Ressources et outils utiles

- Outils :
  - Gestionnaires de mots de passe (Bitwarden, LastPass, Dashlane 🇫🇷, MailinBlack Sikker 🇫🇷)
  - Plateformes de sauvegarde (Google Drive, OneDrive, oodrive 🇫🇷)
- Programmes de soutien :
  - FranceNum : Experts locaux
  - Cybermalveillance.gouv.fr
  - CSIRT-BFC : https://www.csirt-bfc.fr/

1. Gestionnaires de mots de passe

Les mots de passe faibles ou réutilisés sont une porte d'entrée courante pour les cyberattaques. Les gestionnaires de mots de passe permettent de créer et stocker des mots de passe robustes et uniques pour chaque service.

Outils recommandés :

- Bitwarden (gratuit et open source)
- ~~LastPass (freemium)~~
- Dashlane (payant) 🇫🇷
- Sikker (payant) 🇫🇷

Avantage : Propose une authentification multifactorielle pour une sécurité accrue.

2. Plateformes de sauvegarde

En cas de ransomware ou de panne, une sauvegarde régulière garantit que les données critiques peuvent être restaurées rapidement.

Outils recommandés :

- Google Drive (gratuit jusqu'à 15 Go)
- Microsoft OneDrive (freemium)
- Solutions physiques : disques durs externes sécurisés.

Conseil pratique : Adoptez la règle des 3-2-1 : 3 copies des données, sur 2 types de supports différents, dont 1 hors site (cloud ou disque externe).

3. Antivirus et pare-feu

Ils constituent une première ligne de défense contre les logiciels malveillants et les intrusions réseau.

Outils recommandés :

- Avast Free Antivirus (gratuit pour les particuliers, payant pour les entreprises).
- ~~Kaspersky Small Office Security (spécialement conçu pour les TPE).~~
- Bitdefender (freemium).
- Microsoft Defender (natif dans Windows 11)

Bonnes pratiques :

- Activez le pare-feu natif de votre système d'exploitation (Windows/Mac).
- Effectuez des mises à jour régulières pour garder ces outils efficaces.

4. Sensibilisation et formation des collaborateurs

L'erreur humaine est responsable de la majorité des incidents cyber. Former les équipes à identifier les risques est crucial.

Outils recommandés :

- Cybermalveillance.gouv.fr (ressources gratuites de sensibilisation).
- PhishingBox : Simulations de phishing pour tester et former les employés.
- MailinBlack : Plateforme dédiée à la formation et à la sensibilisation.

Astuce : Organisez des sessions régulières pour maintenir une vigilance continue.

5. Outils de vérification et d'analyse de sécurité

Ces outils permettent d'évaluer le niveau de sécurité des systèmes et de détecter des vulnérabilités potentielles.

Outils recommandés :

- Have I Been Pwned : Vérifie si vos emails ont été compromis.
- ShieldsUp : Analyse les ports réseau ouverts pour détecter les failles.
- VirusTotal : Analyse des fichiers suspects pour détecter des malwares.

6. Assistance en cas d'incident

Savoir à qui s'adresser en cas de cyberattaque permet de limiter les impacts et de réagir efficacement.

Ressources utiles :

- Cybermalveillance.gouv.fr : Accompagnement et conseils personnalisés en cas d'attaque.
- ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) : Conseils pour les entreprises.
- ExpertCyber : Annuaire d'experts certifiés pour aider les TPE/PME.

7. Plans de sécurité simples pour TPE/PME

Un plan structuré aide à prioriser les actions de cybersécurité.

1. Évaluation initiale des risques.
2. Mise en place des sauvegardes.
3. Sensibilisation des collaborateurs.
4. Adoption d'un gestionnaire de mots de passe.
5. Intégration d'un antivirus et d'un pare-feu.

Ressources

https://www.proximgroupe.fr/pages/activites/formation/ressources-a-telecharger.html

07 Ressources et outils utiles

Questions / réponses et conclusion

MERCI

Thomas Petit
- 06.82.20.60.50
- thomas.petit@proximgroupe.fr

Proxim CYBERSOLUTIONS

www.proximgroupe.com

Proxim GROUPE