Ils font la cyber en Occitanie
Entretiens avec :
Orange
L'ANSSI
Predicta Lab…
P. 2

le journal de la CYBER

Parlez-vous cyber ?
Quelques définitions P. 2

+ Mots de passe, phishing...
Les conseils de notre expert Ajyle
pour se protéger efficacement P. 3-4

#32* - Avril 2024

Menaces cyber : le Gers contre-attaque !

© Gers Numérique - Adonis Creative - Freepik

GERS NUMÉRIQUE DÉPLOIE SON BOUQUET DE SERVICES

Dans le Gers, le soutien numérique a pris une nouvelle dimension en étendant son action aux communautés de communes et aux communes. Entretien avec Jean-Pierre Salers, président de Gers Numérique.

© Photo officielle - Conseil départemental du Gers

Peut-on dire que le bonheur n'est plus seulement dans le pré, mais aussi dans le numérique ?

Oui, le Gers croit fermement que son avenir passe par le numérique. Le département est très heureux d'accueillir le CyberTour. Gers Numérique est familier de l'événement toulousain, et nous avions donc à cœur de permettre qu'une étape se tienne rapidement à Auch. Ce ne sera une surprise pour personne : Gers Numérique, dont le cœur de métier et la mission principale sont le déploiement d'infrastructures numériques, et en premier lieu du réseau en fibre optique, se penche sur les usages et services numériques. Depuis 3 ans, les 4 conseillers de Gers Numérique parcourent le département pour animer des ateliers ou proposer un soutien individualisé aux habitants mal à l'aise avec la transformation numérique du quotidien, qu'il s'agisse de la prise en main de matériel et d'outils ou de la dématérialisation des démarches administratives.

Votre action privilégie désormais les communes rurales. Parlez-nous de ce « bouquet de services » que Gers Numérique leur propose.

Grâce à un soutien décisif de France Relance et du conseil départemental, Gers Numérique est devenu le levier de mutualisation pour des acteurs publics qui avaient du mal à dédier des moyens humains, matériels et financiers à ces sujets. Qu'il s'agisse d'informatique au sens large, de sauvegarde des données publiques avec l'accès au nouveau data center d'Auch, du développement d'une application de relation avec les citoyens, de système d'information géographique avec l'adressage des petites communes, l'accompagnement de Gers Numérique auprès des collectivités prend de nombreuses formes et s'adapte toujours aux besoins du maire et des agents publics en veillant à ne pas contrarier les habitudes de travail. Naturellement, la cybersécurité fait partie des tout premiers projets engagés dans les mairies.

> **« La cybersécurité n'est pas qu'affaire de technique et de protection : il faut aussi insister sur le facteur humain. »**

Certains seront surpris que la cybersécurité soit à ce point un sujet pour un département rural… Que leur répondez-vous ?

Il y a eu des mairies, des établissements publics et des PME hackés dans le Gers. Le premier objectif de ce CyberTour est évidemment la sensibilisation des élus et des acteurs économiques ; même si l'actualité s'en charge régulièrement. Le sujet peut paraître aussi inquiétant que lointain alors qu'il est bien réel. Les cybervictimes ne sont que très rarement ciblées, et ce n'est pas parce que l'on est une PME ou une mairie dans un vallon gersois que l'on est « trop petit » et donc à l'abri. La suite logique pour Gers Numérique est donc de généraliser un « kit de survie » dans les collectivités publiques pour protéger les messageries, les postes de travail. Pour éviter de solliciter les secrétaires de mairie déjà très occupées, notre équipe réalise ce travail « clés en main » en s'appuyant sur des outils approuvés par l'ANSSI.
La cybersécurité n'est pas qu'affaire de technique et de protection : il faut aussi insister sur le facteur humain. C'est le troisième axe des services proposés par Gers Numérique aux collectivités publiques : les bons réflexes à adopter avant… et même pendant et après une attaque pour en limiter les dégâts.

www.gersnumerique.fr

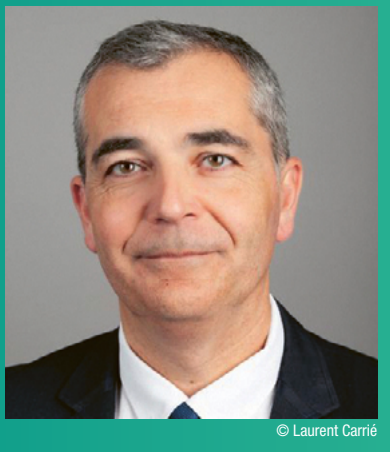
Vous avez dit CyberTour ?

Le CyberTour, organisé par Projet X, est un **programme de conférences locales interactives au format TED**, une plateforme d'échanges et d'apprentissage sur la cybersécurité où pros, experts et novices se rencontrent et partagent leurs expériences. Des **keynotes** et des **tables rondes** rassemblant des intervenants de premier plan ainsi que des **ateliers interactifs** offrent aux participants une compréhension approfondie des défis et des meilleures pratiques.

Cybersécurité : des risques exponentiels, un défi majeur

La transformation numérique a modifié en profondeur les usages et les comportements. **Être connecté est devenu le quotidien.** Les échanges dématérialisés entre les citoyens, les entreprises et les administrations publiques se sont multipliés tant dans les usages personnels que professionnels et n'échappent pas aux activités malveillantes.
La protection des informations créées et stockées doit également être une priorité partagée à tout instant par tous.
En tant que préfet de département, j'ai la responsabilité de coordonner au niveau départemental le dispositif de politique publique de sécurité économique. La cybersécurité en est une des composantes et, à ce titre, des actions sont organisées sous mon autorité régulièrement. Elles ont vocation à se multiplier afin de **mieux accompagner les Gersois pour se prémunir contre le risque cyber et y faire face**.
Aujourd'hui, la question n'est plus de savoir si vous allez être victime ou non d'une cyberattaque mais quand.
Nous avons donc l'obligation de nous y préparer collectivement.

Laurent Carrié
Préfet du Gers



© Laurent Carrié

ORANGE CYBERDEFENSE, FORMER ET PROTÉGER À TOUS NIVEAUX

La filiale de l'opérateur télécom, acteur majeur de la cybersécurité en Europe, emploie 120 experts dans le Sud-Ouest. Entretien avec **Nicolas Brochot**, délégué régional Orange Occitanie.

© Orange

Quelle est la vision d'Orange concernant l'importance du CyberTour pour la communauté de la cybersécurité?

Orange est l'acteur de confiance qui donne à chacune et à chacun les clés d'un monde numérique responsable. Les défis en matière de cybersécurité sont nombreux et cet événement est une opportunité majeure pour sensibiliser les citoyens, les entreprises et les collectivités du territoire du Gers aux enjeux de la sécurité numérique. En tant qu'opérateur télécom, notre objectif est de permettre à tous de profiter des avantages du très haut débit tout en garantissant la protection et la confidentialité des données.

Comment Orange Cyberdefense répond-elle aux principaux défis de cybersécurité que le monde numérique affronte aujourd'hui ?

Dans un contexte de forte croissance des cyberattaques, Orange Cyberdefense a pour mission de venir au secours de nombreux clients qui sont victimes de hackers malintentionnés, avec demandes de rançons à la clé, et toujours plus expérimentés. Pour répondre localement à des besoins en forte croissance, Orange propose à ses clients un service sur mesure, avec des nouvelles offres de surveillance et de protection contre les menaces cyber, qui s'incarnent autour du Micro-SOC, une solution qui permet de protéger les postes de travail et les serveurs d'une entreprise. Son arsenal est complété par des offres innovantes en matière de gestion de crise, sécurité du cloud, environnements industriels et objets connectés, sans oublier des programmes de formation aux risques cyber. Orange a choisi de s'implanter en région car la majorité des attaques touche des TPE, PME et collectivités. Il est donc important d'être présent localement et d'analyser les besoins spécifiques de chacun.

> **La majorité des attaques touche des TPE, PME et collectivités. Il est donc important d'être présent localement.**

Quel rôle Orange Cyberdefense jouera-t-elle pour façonner l'avenir de la cybersécurité ?

L'évolution de la cybersécurité dans les années à venir pourrait inclure une augmentation des attaques basées sur l'intelligence artificielle. Avec la numérisation croissante des services publics, des entreprises et des infrastructures critiques, il est essentiel de garantir la protection des données sensibles et la continuité des activités. Orange Cyberdefense jouera un rôle-clé en développant des solutions de surveillance, de protection des données et de renforcement de la résilience des infrastructures critiques. La sensibilisation et la formation des acteurs des territoires seront prioritaires pour promouvoir la sécurité numérique. Orange Cyberdefense apportera des services pour aider les entreprises et les citoyens à adopter les bonnes pratiques en matière de cybersécurité.

www.orangecyberdefense.com/fr/

AJYLE, CATALYSEUR DE TRANSFORMATION NUMÉRIQUE ET SOCIÉTALE

La société Ajyle accompagne les organisations publiques et privées dans leur parcours de transition numérique. **Samuel Cette**, l'un de ses cofondateurs, nous dévoile son offre.

© Rémy Gabalda - ToulÉco

Quelles sont les spécificités d'Ajyle ?

Nous offrons des formations spécialisées, des conseils stratégiques et un accès à des compétences expertes *via* le modèle des salariés à temps partagé. En mettant l'accent sur l'IA, la cybersécurité et les technologies émergentes, nous dotons nos clients des outils et connaissances nécessaires pour naviguer dans un paysage numérique en constante évolution, donc instable.

> **La mesure de l'efficacité s'envisage, […] cela est unique, sur le suivi longitudinal des incidents de sécurité.**

Comment Ajyle intègre-t-elle les aspects de cybersécurité et de sécurité économique dans ses services de conseil et de formation ?

À travers des formations dédiées, des audits de sécurité et des conseils stratégiques pour renforcer la résilience des organisations face aux menaces numériques, à l'augmentation des attaques ciblées, à l'émergence de nouvelles formes de malwares.

Quelles motivations vous poussent à participer au CyberTour ?

En participant au CyberTour, Ajyle cherche à sensibiliser davantage les organisations aux enjeux de la cybersécurité, partager son expertise, raison pour laquelle nous axons nos interventions sur la transmission d'un message clair et la présentation de solutions concrètes pour y faire face.

Quelle approche adoptez-vous pour former et sensibiliser les organisations et leurs collaborateurs à la cybersécurité et à la sécurité économique ?

Notre approche repose sur des programmes obligatoirement sur mesure, des ateliers pratiques et des séminaires interactifs, conçus pour engager et acculturer les participants. La mesure de l'efficacité s'envisage, certes, à travers des évaluations avant et après formation, des retours d'expérience, mais surtout, et cela est unique, sur le suivi longitudinal des incidents de sécurité.

www.ajyle.fr

PREDICTA LAB, LA PUISSANCE DE L'OSINT

Baptiste Robert est un « hacker éthique » de renommée internationale. Il a cofondé Predicta Lab, une start-up toulousaine spécialisée dans le renseignement en sources ouvertes (OSINT).

Que propose Predicta Lab ?

Notre pôle technique développe des outils d'investigation et de protection des données, tandis que notre pôle d'analyse produit des rapports d'empreintes numériques qui permettent à notre clientèle d'évaluer son exposition en ligne et d'être accompagnée dans la réduction de cette exposition.

Pourquoi participer au CyberTour ?

Chez Predicta Lab, notre mission est de protéger les individus et les organisations contre les menaces numériques en exploitant la puissance de l'OSINT. Nous sommes engagés dans la sensibilisation et la formation à la protection des données. Par ailleurs, étant fièrement toulousains, nous sommes particulièrement enthousiastes à l'idée de participer à cette initiative dans la région Occitanie.

> **Nous sommes engagés dans la sensibilisation et la formation à la protection des données.**

© Predicta Lab

Quelles sont vos actualités ?

Je reviens tout juste de Washington, aux États-Unis, où j'ai représenté Predicta Lab aux côtés de la « CyberTaskForce ». Là-bas, j'ai pu rencontrer et échanger avec les départements de la Justice et de la Défense, ainsi qu'avec la Maison Blanche. Côté innovation, de nouvelles sources sont régulièrement ajoutées à Predicta Search, notre moteur de recherche d'empreinte numérique, et nos développeurs avancent sur Predicta Graph. Cette nouvelle solution de visualisation des données sera bientôt disponible !

www.predictalab.fr

© Christophe Fleury

« Le CyberTour est clairement une *place to be* »

L'ANSSI, agence française de référence en matière de sécurité du numérique, est en charge de promouvoir les bonnes pratiques envers les entités publiques comme privées. **Il faut que les actions de prévention en cybersécurité ruissellent sur le territoire**, et le CyberTour du Gers fait justement partie de ces actions.
Les défis actuels auxquels la France est confrontée tournent autour de la sécurisation des J.O., mais également de la **mise en œuvre de la directive européenne NIS 2**, qui permettra de mieux sécuriser certains domaines, en complément des opérateurs de services essentiels (OSE) et des opérateurs d'importance vitale (OIV). La directive NIS 2 est un changement de paradigme : on passe de quelques centaines d'opérateurs régulés à quelques milliers, ce qui nécessite un passage à l'échelle aussi bien pour les prestataires que pour le régulateur (ANSSI). Cette directive rentrera en application courant octobre 2024 et fait l'objet de consultations vis-à-vis des associations d'élus comme des fédérations métiers.

Christophe Fleury
Délégué à la sécurité numérique pour l'Occitanie – Agence nationale de la sécurité des systèmes d'information (ANSSI)

cyber.gouv.fr/decouvrir-lanssi

Cyber' VOC

- **OSINT (Open Source Intelligence)** : Désigne la collecte et l'analyse d'informations issues de sources publiques pour le renseignement. C'est une pratique utilisée dans la cybersécurité, la sécurité nationale, le journalisme d'investigation et le secteur privé à partir de données issues de médias, de sites web, de bases de données publiques, de réseaux sociaux et d'autres plateformes en ligne.

- **Hacker éthique** : Professionnel de la cybersécurité qui utilise ses compétences pour détecter et corriger les vulnérabilités des systèmes informatiques de manière légale. Son objectif ? Améliorer la sécurité en identifiant les failles avant les cyberattaques. Il agit avec l'autorisation des propriétaires des systèmes.

Dans le vaste univers de la cybersécurité, naviguer à travers les menaces peut s'avérer un défi. Quelques conseils pratiques de notre **expert Ajyle.**

CRÉER UN MOT DE PASSE SÉCURISÉ

C'EST VOTRE PREMIÈRE LIGNE DE DÉFENSE !

Les mots de passe faibles et répétitifs sont l'une des principales failles exploitées par les cybercriminels pour accéder à vos données en ligne. Quelques conseils à suivre !

COMBIEN DE TEMPS POUR CRAQUER VOTRE MOT DE PASSE ? (En 2023)

NOMBRE DE CARACTÈRES	Uniquement des chiffres	Lettres minuscules	Lettres minuscules et majuscules	Lettres minuscules et majuscules + chiffres	Lettres minuscules et majuscules + chiffres + caractères spéciaux
4	immédiat	immédiat	immédiat	immédiat	immédiat
6	immédiat	immédiat	immédiat	3 secondes	5 secondes
8	immédiat	5 secondes	22 minutes	1 heure	5 heures
10	immédiat	58 minutes	1 mois	2 mois	5 ans
12	45 secondes	3 semaines	230 ans	2 000 ans	34 000 ans
14	45 minutes	51 ans	800 000 ans	9 000 000 années	200 000 000 années

LES BONNES PRATIQUES

1. UTILISEZ UN MÉLANGE DE LETTRES, CHIFFRES ET SYMBOLES

POURQUOI C'EST IMPORTANT
L'utilisation d'une combinaison de différents types de caractères rend votre mot de passe beaucoup plus difficile à deviner ou à craquer par des attaques automatisées. Les attaquants utilisent souvent des outils qui génèrent des combinaisons basées sur des mots de passe couramment utilisés, des séquences simples ou des dictionnaires. En mélangeant les lettres (majuscules et minuscules), les chiffres et les symboles, vous créez une barrière supplémentaire contre ces méthodes d'attaque.

COMMENT PROCÉDER
Assurez-vous que chaque mot de passe contient une combinaison aléatoire de majuscules (A-Z), de minuscules (a-z), de chiffres (0-9) et de symboles spéciaux (comme !, @, #, $, etc.). Évitez les séquences prévisibles et les mots complets.

2. CHOISISSEZ UN MOT DE PASSE D'AU MOINS 12 CARACTÈRES

POURQUOI C'EST IMPORTANT
La longueur du mot de passe est un facteur crucial dans sa sécurité. Plus un mot de passe est long, plus le nombre de combinaisons possibles augmente, ce qui rend la tâche de le deviner ou de le craquer extrêmement difficile pour les attaquants.

COMMENT PROCÉDER
Pour vous aider à créer et à retenir des mots de passe longs, vous pouvez utiliser des phrases de passe, qui sont des suites de mots formant une phrase que vous pouvez facilement mémoriser, tout en étant difficile à deviner pour quelqu'un d'autre.

3. ENVISAGEZ UN GESTIONNAIRE DE MOTS DE PASSE POUR LES STOCKER DE MANIÈRE SÉCURISÉE

POURQUOI C'EST IMPORTANT
Avec le grand nombre de comptes en ligne que la plupart des gens possèdent, il devient pratiquement impossible de se souvenir de mots de passe uniques et complexes pour chacun d'eux. Les gestionnaires de mots de passe résolvent ce problème en stockant tous vos mots de passe dans une base de données chiffrée, accessible *via* un mot de passe principal.

COMMENT PROCÉDER
Choisissez un gestionnaire réputé qui offre un chiffrement robuste (comme AES-256). Vous aurez seulement à retenir le mot de passe principal pour accéder à votre coffre-fort de mots de passe. Assurez-vous que celui-ci est extrêmement fort et unique. Ces gestionnaires peuvent également générer des mots de passe forts et uniques pour vous, assurant que chaque compte soit sécurisé au mieux.

57 % des utilisateurs **indiquent noter leurs mots de passe sur un petit papier**

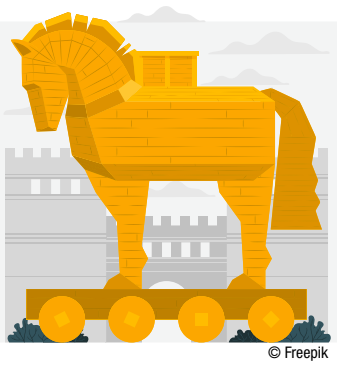
62 % ont déjà **partagé un mot de passe par e-mail**

44 % ont **« recyclé » leur mot de passe** suivant leurs données personnelles

Source : Keeper

UN PEU D'HISTOIRE...

La 1re utilisation documentée d'un mot de passe remonte à l'antiquité, avec le cheval de Troie. Selon le récit, pour s'assurer que seuls les Grecs pouvaient entrer dans le cheval construit pour s'infiltrer dans Troie, les soldats utilisaient un mot de passe en frappant sur la structure selon un code précis.



© Freepik

L'INFO EN +

Et le mot de passe du Wi-Fi ?

Protéger votre réseau domestique est crucial pour la sécurité de vos dispositifs connectés. Une des règles est de **changer le nom par défaut et le mot de passe de votre réseau Wi-Fi**.

Pourquoi ? Parce que les noms (SSID) et mots de passe par défaut des réseaux Wi-Fi sont souvent génériques et peuvent être facilement devinés ou trouvés en ligne. En les modifiant, vous réduisez le risque d'accès non autorisé à votre réseau.

Comment ? C'est très simple :

- Accédez à l'interface administrateur de votre routeur, généralement *via* une adresse IP indiquée sur le routeur ou dans le manuel d'utilisation.
- Recherchez les paramètres Wi-Fi pour changer le SSID (nom du réseau). Choisissez un nom qui ne révèle pas directement votre identité ou votre emplacement.
- Modifiez le mot de passe du Wi-Fi en suivant les bonnes pratiques de création de mots de passe forts et uniques.

ADOPTEZ LES BONS REFLEXES !

Sessions de surf, attention !

On ne le dira jamais assez : quand vous naviguez sur le web, évitez certains comportements qui vous exposent à des **risques importants**, comme utiliser des mots de passe faibles ou identiques, mais aussi **partager des informations personnelles sur des réseaux non sécurisés**. Lorsque vous utilisez des réseaux Wi-Fi publics ou non sécurisés, vos données ne sont pas chiffrées et des individus malintentionnés peuvent potentiellement intercepter les informations que vous envoyez ou recevez, comme vos mots de passe !

Ainsi, il faut :

- Éviter d'utiliser des réseaux Wi-Fi publics pour des transactions ou communications sensibles. Si vous devez absolument vous connecter, envisagez d'utiliser des données mobiles pour des tâches impliquant des informations confidentielles.
- Utiliser un VPN (*virtual private network*) lorsque vous accédez à Internet *via* un réseau public. Un VPN crée un tunnel sécurisé pour vos données, empêchant ainsi les autres utilisateurs du réseau d'intercepter vos informations.
- Vérifier les paramètres de sécurité du réseau avant de vous connecter. Optez pour des réseaux qui exigent un mot de passe et offrent un chiffrement.

(… suite)

LE PHISHING

QU'EST-CE QUE C'EST ET COMMENT L'ÉVITER ?

Le phishing ? Une technique utilisée par les cybercriminels pour vous tromper et vous amener à divulguer des informations personnelles, comme vos mots de passe ou détails bancaires. Ils envoient souvent des e-mails ou des messages qui semblent provenir de sources légitimes.

3 RÈGLES POUR SE PROTÉGER EFFICACEMENT :

1. VÉRIFIEZ TOUJOURS L'ADRESSE E-MAIL DE L'EXPÉDITEUR

POURQUOI C'EST IMPORTANT

Les cybercriminels sont habiles pour masquer leur identité derrière des adresses e-mail qui semblent légitimes à première vue. Ils peuvent utiliser des techniques de spoofing pour faire apparaître leur e-mail comme venant d'une entreprise ou d'une personne de confiance. En inspectant attentivement l'adresse de l'expéditeur, vous pouvez déceler des indices révélateurs, comme des fautes d'orthographe subtiles ou des domaines étrangement formulés, qui indiquent une tentative de phishing.

COMMENT PROCÉDER

- Survolez (sans cliquer) le nom de l'expéditeur pour afficher l'adresse e-mail complète.
- Comparez l'adresse avec celle que vous savez être authentique.
- Soyez particulièrement vigilant avec les e-mails qui demandent des actions urgentes ou des informations personnelles.

2. MÉFIEZ-VOUS DES LIENS ET DES PIÈCES JOINTES DANS LES E-MAILS NON SOLLICITÉS

POURQUOI C'EST IMPORTANT

Les liens et pièces jointes dans les e-mails non sollicités sont des vecteurs courants pour les logiciels malveillants. Cliquer sur un lien ou ouvrir une pièce jointe malveillante peut entraîner l'installation de malwares sur votre appareil, compromettant ainsi votre sécurité et celle de vos données. Ne pensez pas qu'une pièce jointe est forcément un document inerte !

COMMENT PROCÉDER

- Avant de cliquer, survolez le lien pour prévisualiser l'URL et vérifier si elle mène à un site web légitime.
- Évitez d'ouvrir des pièces jointes d'expéditeurs inconnus ou non attendus.
- Si un e-mail semble provenir d'une source fiable mais que vous n'attendiez pas de pièce jointe, contactez l'expéditeur par un autre moyen pour confirmer son authenticité.
- Utilisez des logiciels de sécurité qui incluent une protection contre les liens et pièces jointes malveillants.

3. UTILISEZ LA VÉRIFICATION EN 2 ÉTAPES POUR VOS COMPTES EN LIGNE

POURQUOI C'EST IMPORTANT

La vérification en 2 étapes (également appelée authentification à 2 facteurs ou 2FA) ajoute une couche de sécurité supplémentaire à vos comptes en ligne. Même si un cybercriminel parvient à obtenir votre mot de passe, il lui sera beaucoup plus difficile d'accéder à votre compte sans également avoir accès à votre second facteur d'authentification, qui peut être un code envoyé à votre téléphone, une application d'authentification ou un dispositif matériel.

COMMENT PROCÉDER

- Activez la 2FA sur tous les comptes qui proposent cette option, en particulier sur les comptes critiques tels que les e-mails, les réseaux sociaux et les services bancaires en ligne.
- Préférez les applications d'authentification ou les clés de sécurité matérielles aux SMS ou e-mails, car ces derniers peuvent être interceptés ou détournés.
- Gardez un dispositif de secours configuré pour la 2FA au cas où vous perdriez l'accès à votre principal moyen d'authentification.

UN PEU D'HISTOIRE…

Au milieu des années 1990, on se connectait à Internet *via* un modem. Les pirates, cherchant à obtenir un accès gratuit au web, créaient des programmes qui se faisaient passer pour des logiciels d'authentification légitimes.

DÉFINITIONS

- **Spoofing**

Pratique malveillante visant à se faire passer pour une autre entité ou personne dans le but de gagner la confiance d'une victime, d'obtenir des informations sensibles, de voler des données ou de diffuser des malwares. Cette technique peut être utilisée dans divers contextes, notamment : spoofing d'adresse e-mail, d'adresse IP, d'identifiant d'appelant (*caller ID spoofing*), de site web…

- **Malware**

Logiciel malveillant, conçu pour endommager ou infiltrer un système informatique. Il peut se présenter sous forme de virus, de « ransomware » (qui prend en otage les données et menace de les diffuser si une rançon n'est pas payée) ou de « spyware » (qui espionne l'activité et vole les données).

- **Ingénierie sociale**

Manipulation psychologique des personnes dans le but d'obtenir des informations confidentielles ou d'accéder à des systèmes sécurisés. Les attaquants exploitent souvent la confiance, la curiosité ou la peur des victimes.

L'INFO EN +

Les autres formes de phishing

- **Le phishing à ciblage étroit (*spear phishing*)** vise des individus ou des organisations spécifiques avec des messages particulièrement personnalisés pour augmenter les chances de succès. Exemples : attaques de médias comme celle contre TV5 Monde en 2015, le piratage de la campagne présidentielle française de 2017 ou encore les atteintes à la sécurité des données des hôpitaux.

- **Le hameçonnage vocal (vishing)** est pratiqué par téléphone. Les attaquants utilisent des techniques d'ingénierie sociale pour extorquer des informations personnelles, financières ou de sécurité à leurs victimes, souvent en se faisant passer pour des institutions de confiance. Exemples : l'arnaque au support technique, les fausses alertes de fraude bancaire, les offres d'investissement frauduleuses…

- **Le smishing (*SMS phishing*)** utilise les messages texte comme vecteurs d'attaque pour tromper les destinataires en leur faisant divulguer des informations sensibles ou en les poussant à cliquer sur des liens malveillants *via* leur téléphone mobile.

Le *Journal de la cyber* est édité par **Projet X** - N° 32 (* numéro bêta) – avril 2024
Directeur de la publication : Samuel Cette
Comité éditorial : Jean-Christophe Arguillère, Samuel Cette, Célie Cousinié, Ingrid Gautier, Martin Venzal
Rédaction, création graphique et maquette : Adonis Créative – **Impression :** Techni Print imprimerie