Protéger votre TPE/PME des cyberattaques

Comprendre et agir

QI YANG

Micro-entrepreneurs, dirigeants de TPE-PME,

la menace informatique vous concerne vous aussi. Il existe des moyens faciles de vous en protéger.

Si le risque cyber est connu de longue date (la première attaque informatique remonte à 1988), la menace ne cesse d'évoluer et de se complexifier. Au fil des années, les cybercriminels ont su améliorer leur capacité et se professionnaliser de manière constante, ce qui est à la fois « une cause et une conséquence de la maturité et des gains financiers acquis par ses acteurs » selon l'ANSSI. Des gains estimés à plus d'un milliard d'euros par an[1].

" L'encourageant ralentissement du nombre d'incidents constaté pour nos clients les plus matures montre que nous sommes capables de remporter des batailles contre les acteurs malveillants "

Hugues Foulon, directeur général d'Orange Cyberdefense.

Les pirates informatiques innovent sans cesse et tirent parti de la moindre opportunité, tels que l'explosion du télétravail et la généralisation d'usages numériques parfois mal maîtrisés. 2020-2021 se distingue aussi par l'explosion du nombre de vulnérabilités 0-Day exploitées[2], c'est-à-dire ces failles détectées dans un logiciel ou un système d'exploitation qui n'ont pas encore été traitées par les éditeurs.

Or, ces attaques ne sont pas sans conséquences pour les entreprises visées : activité mise à l'arrêt, pertes financières, vol de données, perte de confiance des clients…

Dans ce contexte, les entreprises doivent se mobiliser et s'adapter en permanence. Des solutions techniques existent et doivent être déployées pour sécuriser les systèmes informatiques. Pour autant, la première ligne de défense reste l'humain.

Car il s'agit bien là du maillon faible. Par des usages inappropriés, par négligence ou par manque d'information, les utilisateurs sont ceux qui ouvrent le plus souvent la porte aux cybercriminels. Heureusement, vous pouvez mettre en place des actions très simples pour y remédier, que vous soyez entrepreneur solo ou dirigeant d'une TPE-PME.

C'est l'objet de ce livre blanc conçu pour vous donner toutes les clés pratiques pour protéger au mieux votre entreprise.

x4,5

Les petites entreprises sont 4,5 fois plus nombreuses à être victimes de cyber-extorsion que les moyennes et grandes réunies[3].

49%

Pourcentage d'entreprises françaises ayant signalé une cyberattaque en 2021 (contre 34 % l'année précédente). 22 % des entreprises françaises ciblées ont subi plus de 25 attaques[4].

6/10

Nombre d'entreprises françaises victimes qui déclarent, en 2021, avoir subi un impact sur leur activité, avec, en premier lieu, une perturbation de la production (21 %), une compromission d'information (14 %) et une indisponibilité de leur site web (14 %)[5].

1/6

Proportion, à l'échelle mondiale, des entreprises victimes d'une attaque ayant déclaré avoir risqué de peu la faillite[6].

[1] et [2] Agence nationale de la sécurité des systèmes d'information, « Panorama de la menace informatique 2021 ».

[3] Orange Cyberdefense, Rapport « Security Navigator 2023 ».

[4] Rapport Hiscox 2021 sur la gestion des cyber-risques.

[5] 7e Baromètre annuel du Cesin, Enquête sur la cybersécurité des entreprises françaises.

[6] Rapport Hiscox 2021 sur la gestion des cyber-risques.

01

Cyberattaques : de quoi parle-t-on ?

Lumière sur les principales menaces

Les rançongiciels

Principe

Un rançongiciel (ou « ransomware ») vise à extorquer des fonds par le biais d'un logiciel de cryptage bloquant l'accès à un ordinateur et aux données qu'il contient, en attendant le paiement d'une rançon.

Depuis peu, certains pirates informatiques ajoutent une pression supplémentaire en menaçant de rendre publiques les informations collectées.

En pratique

Un artisan dans l'Est de la France a été victime d'une attaque sur ses logiciels de comptabilité et de caisse. Les malfaiteurs demandaient une rançon de plusieurs centaines de milliers d'euros pour les débloquer.

Son activité fut contrainte de tourner au ralenti (avec des encaissements manuels), sans compter le coût de la remise en état de son réseau informatique devenu inexploitable.

Près d'1 sur 5

Nombre d'entreprises ayant déjà fait l'objet d'une attaque par rançongiciel*.

52%

Proportion de TPE-PME-ETI parmi les entités victimes d'attaques par rançongiciels en 2021 (vs 34 % en 2020).**

** Rapport Hiscox 2022 sur la gestion des cyber-risques.*

*** ANSSI, « Panorama de la menace informatique 2021 ».*

L’hameçonnage

Principe

L’hameçonnage (ou « phishing ») consiste pour les malfaiteurs à envoyer un mail, un SMS ou encore un message via les réseaux sociaux en se faisant passer pour un tiers de confiance (organisme public, partenaire commercial…).

Objectifs : récupérer vos données (identifiants et mots de passe, coordonnées bancaires…) et modifier vos codes pour prendre la main sur vos applications, procéder à un transfert d’argent ou accéder à vos données clients ; propager un rançongiciel ou tout autre programme malveillant, etc.

En pratique

Le salarié d’une TPE située dans le sud-ouest de la France a reçu un mail l’invitant à se connecter à l’un de ses outils métiers pour y mettre à jour des informations.

Les hackers ont intercepté son identifiant et son mot de passe qui se trouvaient être identiques à ceux de sa messagerie professionnelle et d’autres applications. Il leur a suffi d’accéder à sa boîte et d’envoyer de fausses factures. Pour passer inaperçus le plus longtemps possible, des règles de classement et d’archivage des réponses avaient été mises en place.

L’arnaque au virement bancaire

Principe

On parle aussi d’escroquerie aux faux ordres de virement (FOVI) ou de fraude au président.
Ici, les malfaiteurs se font passer pour un fournisseur souhaitant communiquer de nouvelles coordonnées bancaires.

Ils peuvent aussi usurper l’identité d’un dirigeant d’entreprise ou d’un avocat missionné pour le compte de la société qui exige un virement présenté comme urgent et confidentiel.
Ce type d’arnaque s’appuie sur analyse des informations disponibles sur internet et les réseaux sociaux ou après un piratage de données (via une campagne de phishing par exemple).

En pratique

La secrétaire d’une petite entreprise dans l’ouest de la France a reçu des appels de personnes se faisant passer pour un client et un fournisseur. Les malfaiteurs ont réussi au fil des échanges à se faire communiquer le nom du comptable et de la banque de la société ainsi que l’adresse e-mail du dirigeant. Ils ont pu dès lors entrer en contact avec le comptable, en utilisant par ailleurs le nom et l’en-tête de cabinets d’avocats et comptables bien réels (mais renvoyant vers un faux numéro).

Au final, ils sont parvenus à se faire virer environ 100 000 euros.

+ de 4500

Nombre d’escroqueries ou tentatives d’escroqueries recensées depuis 2010, visant des entreprises implantées en France ou des filiales domiciliées à l’étranger*.

+ d’1 Md €

Montant total des préjudices subis*.

** Task force nationale de lutte contre les arnaques, « Guide de prévention contre les arnaques », édition 2022.*

L’attaque par déni de service ou déni de service distribué

Principe

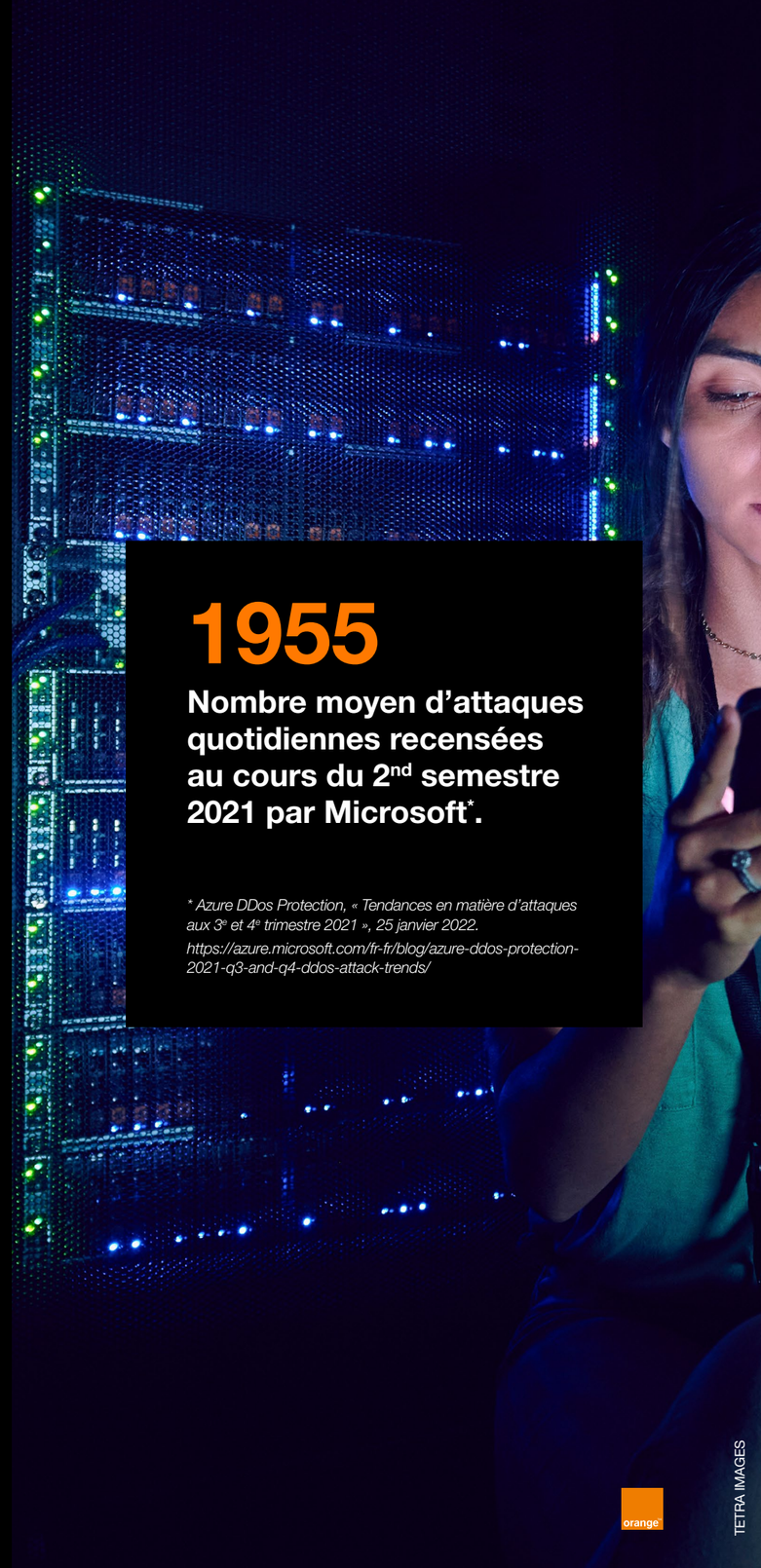
Il s’agit ici de surcharger la bande passante d’un serveur par l’envoi massif de requêtes ou bien par l’exploitation d’une faille informatique dans le but de provoquer la panne ou le ralentissement d’un service, et dans certains cas de demander une rançon.

Ce type d’attaque est redoutable pour l’image de l’entreprise, car visible à l’externe, aux yeux entre autres des clients.

En pratique

Une PME localisée dans la région Grand Est a reçu des menaces d’attaques en déni de service dans lesquelles il lui était demandé de verser une rançon de plusieurs milliers d’euros.

Faute de paiement, l’attaque est finalement déclenchée. Elle a paralysé le site e-commerce de l’entreprise pendant plusieurs jours, avec un impact sur le chiffre d’affaires.



1955

Nombre moyen d’attaques quotidiennes recensées au cours du 2nd semestre 2021 par Microsoft*.

** Azure DDos Protection, « Tendances en matière d’attaques aux 3e et 4e trimestre 2021 », 25 janvier 2022. https://azure.microsoft.com/fr-fr/blog/azure-ddos-protection-2021-q3-and-q4-ddos-attack-trends/*

TETRA IMAGES

Ils constituent des références !

Une question ? Besoin d'informations ? Vous pouvez vous rapprocher de ces organismes publics, acteurs incontournables de la cybersécurité en France.

L'ANSSI

L'Agence nationale de la sécurité des systèmes d'information apporte son expertise technique aux administrations et aux entreprises, en particulier auprès des opérateurs d'importance vitale (OIV). Elle sensibilise, accompagne et forme les entreprises de toute taille aux enjeux de cybersécurité.
https://www.ssi.gouv.fr/

Cybermalveillance.gouv.fr

Il s'agit du dispositif national d'assistance aux victimes d'actes de cybermalveillance. En tant qu'entreprise, vous y trouverez aussi au quotidien de nombreuses informations sur les menaces numériques et les moyens de s'en protéger.
https://www.cybermalveillance.gouv.fr/

Les impacts d’une cyberattaque

Coûts financiers
Directs

- Enquêtes techniques
- Notification client
- Sécurisation des données et des équipements
- Bad buzz sur les réseaux sociaux
- Perte de confiance des clients et des partenaires

Image de l’entreprise

Coûts financiers
Indirects

- Perte de CA suite au ralentissement ou à l’arrêt de l’activité
- Investissement pour renforcer la sécurité de vos installations

Risque juridique

En cas de violation de données, des sanctions possibles pour l’entreprise et son dirigeant, en application du RGPD qui définit la responsabilité des acteurs des traitements de données.

Coût moyen d’une cyberattaque pour une TPE/PME

7273€

pour les entreprises de moins de 10 salariés*

**Source : Rapport Hiscox 2021 sur la gestion des cyber-risques*

Le RGPD, c’est quoi ?

Le Règlement général sur la protection des données (RGPD) encadre le traitement des données personnelles au sein de l’Union européenne.

Vous êtes concerné, quelles que soient la taille et l’activité de votre entreprise, dès lors que vous traitez des informations qui permettent d’identifier ou de rendre identifiable une personne physique (nom, prénom, numéro de téléphone…).

+ d’infos sur le site internet de la CNIL.

02

Se protéger, mode d’emploi

Mesure pouvant présenter un coût

Mesure applicable à partir d’un salarié ou plus.

Mesure applicable sur ordinateur

Mesure applicable sur smartphone

Protégez vos postes de travail

Téléchargez vos logiciels uniquement depuis les sites officiels des éditeurs

Au-delà des questions de légalité, c'est la certitude de ne pas télécharger de logiciels contenant des virus ou des chevaux de Troie qui pourraient endommager vos équipements, prendre le contrôle de vos postes informatiques à distance, voler des données, etc.

Vous serez certain par ailleurs de bénéficier des mises à jour effectuées régulièrement par les éditeurs.

Installez les mises à jour de sécurité

Aussi bien celles de vos systèmes d'exploitation (Windows, macOS, Android…) que de vos logiciels.

Ces mises à jour ont pour but de corriger les failles informatiques éventuellement identifiées par les éditeurs.

Pour éviter tout oubli, configurez leur téléchargement automatique depuis les paramètres de votre ordinateur et de vos logiciels.

Chiffrez les données et fichiers sensibles, en particulier avant de les sauvegarder

Cette protection sera utile si un malfaiteur parvient à mettre la main sur vos appareils (dont vos supports de sauvegarde).

Vous trouverez des outils gratuits en ligne, dont certains recommandés par la CNIL, comme 7-Zip, Peazip, VeraCrypt, Zed !

Dotez-vous d'une solution de protection contre les menaces numériques

Alors que des centaines de milliers de codes malveillants apparaissent chaque jour, programmez un scan automatique de vos machines, des fichiers téléchargés et des périphériques externes, depuis les paramètres de votre ordinateur ou de votre antivirus.

Cet outil, complémentaire au pare-feu, analysera automatiquement votre appareil pour détecter tout fichier suspect et le mettre en quarantaine le cas échéant.

Chez Orange, nous avons la solution qu'il faut !

Pour se prémunir des cyberattaques de type malware, **Cyber Protection**, une solution conçue par Orange, combinant intelligence artificielle et humaine assure une protection des données et des équipements de l'entreprise 24/7.

Protégez vos postes de travail

Organiser la sauvegarde régulière de vos données sur un support externe

L'objectif est de garantir la continuité de votre activité en cas d'attaque ou de dysfonctionnement. Pour cela :

- Dressez l'inventaire de vos données, sans oublier celles contenues sur votre smartphone.
- Choisissez votre support de sauvegarde. Par exemple, un disque dur externe (veillez à bien le déconnecter de votre réseau une fois la sauvegarde terminée), ou bien une solution cloud.
- Configurez une sauvegarde automatique régulière depuis les paramètres de votre ordinateur (dont vous vérifierez régulièrement le bon fonctionnement).

Activez les pare-feux sur vos appareils

Cet outil contrôlera de manière préventive l'ensemble du trafic internet sur votre réseau et interceptera en temps réel toute connexion malveillante.
Selon le niveau de sécurité attendu, vous pouvez utiliser celui préinstallé par défaut sur votre appareil ou souscrire à une suite logicielle tierce.

Remplacez les matériels et logiciels trop anciens

Ils ne bénéficient plus des mises à jour de sécurité.

Limitez les applications téléchargées sur votre smartphone

Avant toute installation, soyez attentif à la liste des données auxquelles elles accéderont. Certaines applications demandent des autorisations d'accès exagérées par rapport à l'usage que vous prévoyez d'en faire.

Il est primordial de ne pas négliger la cybersécurité de votre entreprise, le recours à un antivirus professionnel est une première action indispensable.

Nicolas, expert cybersécurité chez Orange.

PETER CADE - MORSA IMAGES

Les accès numériques et physiques

Choisissez des mots de passe forts

Pour accéder à vos données, les pirates informatiques peuvent se montrer très patients et tester toutes les combinaisons possibles jusqu'à trouver le sésame. Alors, plus vous opposerez des mots de passe complexes à ces attaques dites « par force brute », plus les hackers auront besoin de temps pour parvenir à leurs fins, plus vous aurez de chance de les détecter.

Plus concrètement :

- Changez systématiquement les mots de passe attribués par défaut. Vous noterez qu'il n'est plus conseillé de changer tous vos mots de passe régulièrement (des études montrant que les utilisateurs avaient alors tendance à choisir des mots de passe plus prédictibles) mais plutôt lorsque nécessaires (vous suspectez une attaque par exemple).

- Choisissez un mot de passe contenant au moins 12 caractères et comprenant à la fois des majuscules, des minuscules, des chiffres et des caractères spéciaux.

- Évitez les mots de passe trop évidents : votre nom ou celui de vos enfants, une date de naissance…

- Ne choisissez pas de noms communs ou d'expressions connus (« azerty » par exemple). Une méthode efficace consiste notamment à choisir une phrase puis à utiliser les premières lettres de chaque mot.

- Utilisez un mot de passe propre à chaque application pour ne pas remettre la clé de tous vos comptes aux pirates informatiques.

Ne préenregistrez pas les mots de passe dans votre navigateur internet et vos applications et bien sûr, ne les notez pas sur des bouts de papier. Si vous craignez de les oublier, faites plutôt le choix « coffre-fort » de mot de passe (de préférence certifié par l'ANSSI).

Les accès numériques et physiques

Organisez la circulation au sein de vos locaux

Prévoyez l'accueil de vos clients et fournisseurs afin de ne pas les laisser seuls dans vos locaux. Le cas échéant, sécurisez la porte conduisant à la salle qui abrite vos serveurs en la fermant à clé ou en installant un verrou à code par exemple.

Utilisez votre session administrateur à bon escient

Connectez-vous via votre session Administrateur uniquement quand vous avez besoin d'agir sur le paramétrage de votre poste.

Une session utilisateur suffit largement pour vos usages professionnels quotidiens.

Pour tous vos logiciels et outils métiers, créez un compte utilisateur par salarié

Interdiction de partager vos codes ! Chacun doit disposer d'un identifiant et d'un mot de passe personnels, le plus fort possible (voir page 13). C'est le moyen de contrôler les accès de chacun aux différentes ressources métiers.

Assurez-vous, pour chacun de vos salariés et prestataires, que leurs droits d'accès à votre réseau et à vos outils métiers correspondent bien à leurs besoins

Le stagiaire a-t-il besoin des droits les plus élargis sur votre logiciel de comptabilité ? Votre gestionnaire RH, parti en retraite, a-t-il toujours besoin d'un accès à votre outil de paie ?

Mettez en place une procédure qui prévoit la fermeture des comptes après chaque départ ou leur ajustement dans le cas d'un changement de poste.

Protégez vos données en ligne

Elles pourraient être exploitées par des personnes malintentionnées pour en déduire vos mots de passe, espionner votre activité ou encore usurper votre identité. Autrement dit :

- Soyez vigilant quant aux informations publiées sur vos réseaux sociaux, a fortiori lorsqu'elles sont publiques.
- Dans les formulaires en ligne, ne communiquez que les informations strictement obligatoires.
- Ne donnez pas votre accord pour la conservation de vos données personnelles et leur partage avec des partenaires commerciaux.

Votre réseau Internet

Protégez l'accès à l'interface de configuration de votre box

Personnalisez le nom d'utilisateur et le mot de passe communiqués à l'ouverture de votre contrat.

Vérifiez le niveau de sécurité de votre Wi-Fi

Pour cela, rendez-vous dans l'interface de configuration de votre box en saisissant dans votre navigateur l'url communiquée par votre fournisseur Internet.

Assurez-vous que le protocoleWPA2 est activé (ou WPA3, pour les routeurs les plus récents) afin de bénéficier du plus haut niveau de cryptage de vos données.

Changez votre clé de connexion Wi-Fi

Cette précaution est particulièrement utile si vous êtes amené à partager votre clé (avec des clients de passage dans vos locaux par exemple).

Votre clé doit compter au moins 20 caractères et combiner des majuscules, des minuscules et des chiffres.

Contrôlez régulièrement les connexions Wi-Fi à votre réseau

Vous pouvez accéder à la liste des utilisateurs connectés à votre Wi-Fi via votre interface de connexion.

Le cas échéant, bloquez l'intrus et profitez-en pour changer votre clé de connexion (qui a visiblement été craquée).

Offrir du Wifi à ses clients est devenu un service à part entière. Vous pouvez proposer une solution qui garantisse la sécurité de votre réseau et de vos données.

Nicolas, expert cybersécurité chez Orange.

Chez Orange, nous avons les solutions qu'il faut !

Wifi Guest vous permet d'offrir un accès Wifi performant et sécurisé à vos visiteurs et clients tout en vous protégeant des intrusions.

Vos usages en mobilité

Évitez toute connexion aux réseaux Wi-Fi publics et branchement aux bornes de recharges en libre accès

Le principal risque ici est de voir ses données interceptées par des pirates informatiques ou de télécharger un virus informatique.

Installez un filtre de confidentialité sur votre écran d'ordinateur.

Il devient impossible de lire ce qui est affiché sur votre écran, à moins de se trouver directement face à lui.

Configurez un VPN

Le réseau privé virtuel (ou « virtual private network », VPN) consiste à chiffrer les informations qui transitent entre vous et le réseau internet, y compris si vous utilisez un réseau Wi-Fi public. Pour en profiter, il vous faudra souscrire à ce service auprès du fournisseur de votre choix et installer une application sur vos appareils.

En cas de déplacement à l'étranger

Évitez de partir avec des données sensibles dans votre ordinateur. Essayez de ne prendre avec vous que les fichiers indispensables à votre voyage. Faites une sauvegarde avant de partir. Changez vos mots de passe au retour.

Désactivez le Bluetooth et le Wi-Fi de vos appareils si vous n'en avez pas besoin

Vous éviterez toute connexion, à votre insu, d'appareils malveillants localisés à proximité.

Utilisez uniquement des appareils de confiance, à savoir les vôtres

Ne connectez pas la clé USB d'une tierce personne sur votre ordinateur. Elle pourrait contenir des logiciels malveillants.

Ne laissez jamais vos équipements sans surveillance

Verrouillez votre ordinateur et votre smartphone si vous devez vous éloigner.

Le filtrage DNS est une solution de protection qui peut empêcher le réseau de votre entreprise d'être infecté par des logiciels malveillants et vous protéger contre d'autres cyberattaques, comme le phishing. C'est un excellent moyen pour vous prémunir contre ces menaces et ainsi renforcer la protection informatique de votre entreprise.

Nicolas, expert cybersécurité chez Orange.

Chez Orange, nous avons les solutions qu'il faut !

Cyberfiltre vous aide à naviguer sur Internet et Google avec votre smartphone sans craindre de subir une attaque web qui nuirait à l'intégrité de votre entreprise et à vos performances. Grâce à sa technologie de détection préventive de la menace, l'attaque est bloquée avant d'être téléchargée sur votre smartphone, et ce aussi bien sur le réseau mobile, que le WiFi (avec **Cyberfiltre Avancé**).

HOBO_018 - MORSA IMAGES

Votre messagerie

Mettez en place une procédure de double authentification

Vous augmenterez la sécurité de votre compte en imposant deux formes d'identification à toute connexion : par exemple, la saisie d'un mot de passe et d'un code reçu par SMS.

Si cette option est proposée par votre opérateur, cette option est généralement activable depuis les paramètres de votre messagerie.

En cas de doute, contactez directement votre interlocuteur par téléphone

N'utilisez pas les coordonnées fournies dans le message mais effectuez votre propre recherche.

Ne cliquez pas sur les liens et pièces jointes d'un message qui vous semble suspect

Par exemple, vous ne connaissez pas l'expéditeur d'un mail ? Le contenu vous semble inhabituel (intitulé de fichier ou de lien qui ne correspond pas à l'objet du message, information qui n'a pas lieu d'être envoyée par votre correspondant) ?

Ne partagez aucune information sensible par mail

Ne communiquez jamais de mots de passe, de codes confidentiels, de coordonnées bancaires par mail.

Certains signes simples peuvent vous aider à identifier une tentative de phishing : fautes d'orthographe dans le message, incohérences dans les adresses électroniques, les liens et les noms de domaine, pièces jointes suspectes, messages inhabituellement urgents, demande de paiement, etc.
Soyez vigilant !

Nicolas, expert cybersécurité chez Orange.

Vos usages pros/persos

Créez deux sessions pro/perso si vous travaillez sur un seul et même ordinateur (avec des identifiants de connexions différents)

Le plus sûr étant de travailler depuis des postes de travail distincts, si vous le pouvez.

Dans tous les cas, l'objectif est de compartimenter les usages afin de garantir la confidentialité de vos données respectives.

Distinguez bien vos messageries personnelles et professionnelles

Évitez les transferts de mails : vous prendriez le risque de communiquer des informations sensibles à un contact personnel par erreur. Par ailleurs, les messageries personnelles offrent une sécurité moins élevée que celles pros.

Proscrivez tout usage de votre cloud privé à des fins professionnelles

Leur niveau de sécurité est là aussi moins élevé que leurs équivalents pros.

Pour concilier vos usages professionnels et personnels en toute sécurité, depuis un seul et même terminal, il vous faudra opter l'eSIM (embedded SIM) c'est à dire une carte SIM intégrée dans certains téléphones et dans les montres connectées cellulaires.

Nicolas, expert cybersécurité chez Orange.

Chez Orange, nous avons les solutions qu'il faut !

Pour activer l'eSIM de votre smartphone compatible, et profiter du meilleur réseau mobile, il vous suffit de faire une demande de renouvellement carte SIM vers eSIM depuis votre **Espace client Orange**.

(Se) former aux enjeux de cybersécurité

Mettez en place une veille d'information

Newsletters, alertes… : les hackers innovent en permanence. Mettez sans cesse à jour vos connaissances en matière de sécurité informatique.

Simulez des attaques informatiques

Vous trouverez en ligne des outils pour organiser de fausses campagnes de phishing par exemple. Un bon prétexte pour tester la maturité numérique de vos salariés et engager la discussion autour des réflexes à acquérir.

Sensibilisez et formez vos salariés sur les bonnes pratiques en matière de cybersécurité

Formation de groupe, inscription (parfois gratuite) à des MOOC, informations dispensées lors de réunions d'équipe ou par le biais de mail… : vous avez le choix!

Rédigez une charte informatique

Détaillez-y les bonnes pratiques numériques : règles d'utilisation d'internet et de la messagerie, de téléchargement et d'installation de logiciels et de périphériques… Il convient aussi d'y rappeler la procédure à suivre en cas d'attaque. Remettez ce document à chaque nouvel arrivant dans l'entreprise.

S'assurer contre le risque cyber

Selon les compagnies, les assurances cyber vous donnent accès à un service d'assistance dédié en cas d'attaque. Différents sinistres peuvent aussi être pris en charge : frais liés à la récupération des données compromises, à la réinstallation de vos équipements ou encore à la restauration de votre site web ; perte de revenus liés à une interruption d'activité ; coût des notifications aux victimes ; frais d'intervention d'un expert informatique ou d'un avocat…

Pour évaluer l'intérêt d'une telle solution pour votre entreprise, demandez plusieurs devis. Prenez surtout le temps d'étudier le détail des garanties ainsi que les exclusions prévues au contrat.

03

Face à l'incident

MORSA IMAGES

Check list : l'incident est en train de se produire

Certains signaux doivent vous alerter : ralentissement ou redémarrage inexpliqué des postes de travail ? Surconsommation de bande passante, notamment la nuit ? Disparition ou modification de fichiers, ou à l'inverse apparition de logiciels inconnus ? Apparition de nouveaux comptes administrateurs ?
Une attaque informatique est peut-être en train de se produire.

☑ Dès que possible :

- **Débranchez d'internet et du réseau local les ordinateurs et équipements informatiques infectés.** Vous bloquerez la propagation de l'attaque et les malfaiteurs n'auront plus de moyen d'accès et de contrôle à vos machines.
- **Ne les éteignez pas et ne les redémarrez pas non plus.**
- **Prévenez votre prestataire informatique** si vous en avez un ou contactez le dispositif d'assistance aux victimes d'actes de cybermalveillance (cybermalveillance.gouv.fr).

En cas de demande de rançon, ne payez jamais.

☑ Dans les heures et jours qui suivent (par ordre chronologique) :

- **Déposez plainte auprès de la Police ou de la Gendarmerie** avant toute réinstallation de vos appareils. Il est essentiel pour les forces de l'ordre de disposer de toutes les preuves techniques de l'incident.
- **Essayez d'identifier la menace et de cerner son étendue** pour avoir une bonne vision des actions à déployer en priorité : origine possible de l'intrusion, matériels concernés, données compromises, etc. ? Pour cela, aidez-vous de l'outil de diagnostic en ligne proposé gratuitement par la plateforme Cybermalveillance.gouv.fr, qui vous mettra en relation selon les cas avec un prestataire spécialisé. Vous pouvez aussi vous rapprocher de votre Chambre de Métiers et de l'Artisanat (CMA) ou votre Chambre de Commerce et d'Industrie (CCI).
- **Prévenez votre banque** si des données permettant des transferts de fonds vous ont été dérobées, voire faites immédiatement opposition si vous avez communiqué des coordonnées bancaires dans le cadre d'un hameçonnage par exemple.
- **Déclarez le sinistre auprès de votre assureur** si vous avez souscrit un contrat contre les risques cyber.
- **Notifiez la CNIL** si des données à caractère personnel ont été consultées, modifiées ou supprimées, dans les 72 h qui suivent la constatation de la violation. Il s'agit là d'une obligation légale prévue dans le cadre du RGPD. La CNIL pourra, après examen de l'incident, vous imposer d'informer les personnes concernées si cela n'a pas déjà été fait.

☑ Une fois l'attaque sous contrôle et le travail des enquêteurs terminés :

- **Restaurez les paramètres d'usine de vos appareils.**
- **Relancez vos équipements grâce à vos sauvegardes antérieures à l'incident.**
- **Changez tous vos mots de passe.**
- **Téléchargez les dernières mises à jour de vos logiciels.**

Nota bene :
bien que dans une situation d'urgence, essayez de noter tous les événements et actions mis en œuvre. Conservez le plus de preuves possible de l'attaque (mails reçus, captures ou photos d'écran…).
Le moment venu, toutes ces informations seront précieuses pour les enquêteurs.

Communiquer en cas de cyberattaque


L. ALVAREZ

1 Ne communiquez pas trop tôt … ni trop tard !

Il est important d'avoir une vision claire de la situation avant de prendre la parole :

- Quelle est la nature de l'attaque ?
- Quelles en sont les cibles (internes, externes…) et les impacts identifiés ?
- L'attaque est-elle sous contrôle ?

Pour autant, si vous décidez de communiquer, mieux vaut ne pas trop attendre au risque que l'information ne fuite, ce qui pourrait laisser croire que vous tentiez de dissimuler l'incident.

L'enjeu est de taille : préserver la confiance de vos clients et l'image de votre entreprise.

2 Identifiez les personnes à informer

Prévenez dès que possible les personnes (clients, partenaires…) dont les données ont été ou pourraient être compromises.

Si l'incident a des répercussions visibles à l'externe (site e-commerce indisponible par exemple en raison d'une attaque par déni de service), il peut être pertinent de communiquer via les réseaux sociaux.

Dans l'urgence de la crise, n'oubliez pas de tenir informés vos salariés (si vous en avez)!

3 Tirez les leçons de cette crise… et faites-le savoir !

À l'issue de la crise, vous aurez certainement identifié des mesures correctives à mettre en place. N'hésitez pas à tenir vos clients et partenaires informés pour restaurer/entretenir la confiance.

4 Faites preuve de transparence et de pédagogie

Présentez les faits le plus clairement possible et évitez le jargon informatique si vous vous adressez au grand public. L'objectif est d'éviter de faire naître un sentiment de suspicion qui pourrait provoquer des dommages irréparables sur votre réputation.

Rassurez vos interlocuteurs sur les actions déployées pour mettre fin à l'incident. Prévenez-les des démarches à opérer de leur côté (changement de mot de passe…).

Pour aller plus loin

Les ressources à disposition

https://secnumacademie.gouv.fr/

Le MOOC de l'ANSSI pour vous former gratuitement à la cybersécurité et apprendre à protéger vos outils numériques professionnels.

https://www.cybermalveillance.gouv.fr/

Un site crée par l'ANSSI et le ministère de l'Intérieur, où sont rassemblées toutes les bonnes pratiques pour vous protéger des risques cyber. Vous y trouverez aussi, en cas d'attaque, un outil de diagnostic et des conseils personnalisés

https://www.ssi.gouv.fr/entreprise/

Le site de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui propose de nombreux guides pédagogiques à destination des entrepreneurs.

https://autodiag.orangecyberdefense.com/bsa2/

Un outil proposé par Orange Cyberdéfense pour évaluer votre niveau de sécurité informatique.

https://www.cert.ssi.gouv.fr/

Le site du Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques, pour suivre l'actualité de la cybersécurité sous un angle technique.

Orange, c'est bien plus qu'un opérateur !

La cybersécurité est un enjeu capital pour les entreprises, quelle que soit leur taille, c'est pour cela qu'il est important d'être **bien conseillé et bien accompagné.**

Orange propose aux professionnels de nombreux conseils pratiques, actualités et des offres adaptées **pour protéger et sécuriser votre entreprise des cyberattaques.**

Rendez-vous sur

https://boutiquepro.orange.fr/securite