Si vous avez des difficultés à visualiser cet email, suivez ce lien

- N° 4 -

AU SOMMAIRE - Sécurité des données

ATTENTION A LA FRAUDE

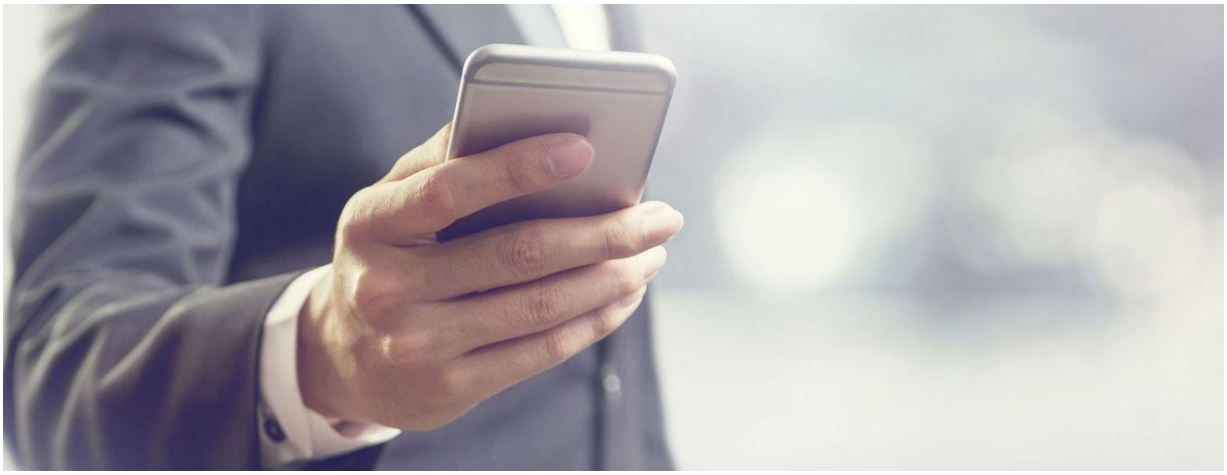
Dans un contexte de télétravail lié à la crise sanitaire, les entreprises sont plus fragilisées et les fraudeurs profitent de cette situation pour attaquer.

Selon l'étude EULER HERMES -DFGC 2020, plus d'1 entreprise sur 4 a été victime d'une fraude avérée en 2019 avec un préjudice supérieur à 10k€ pour 30% d'entre elles et supérieur à 100k€ pour une entreprise sur 10. Dans 48% des cas, la fraude correspondrait à une fraude au faux fournisseur et dans 38% une fraude au président.

EN QUOI CONSISTENT CES FRAUDES ?

Ces deux types de fraudes sont des cas typiques d'abus de confiance. Elles s'appuient sur la connaissance que les fraudeurs ont de l'entreprise (son mode de fonctionnement, ses interlocuteurs…), sur la mise en place d'un scénario crédible et sur leur capacité à contrôler psychologiquement la personne qui, malgré elle, va devenir leur complice.

Dans le cas de la fraude au faux fournisseur, le fraudeur bien renseigné sur les fournisseurs de l'entreprise les appelle en se faisant passer pour le comptable de l'entreprise et demande quelles sont les factures en attente de paiement. Ensuite, il inverse le schéma, il se fait passer pour le fournisseur et appelle le service comptable de l'entreprise en prétextant un changement de compte bancaire pour payer les factures en attente. Il donnera bien évidement les détails sur les factures dues (montant, numéro de factures…) et sera parfois même en capacité de les présenter s'il a pris soin de demander des copies au fournisseur. Le comptable ne se méfiant pas, procède au changement de RIB. La fraude ne sera détectée que lorsque le fournisseur, le vrai, réclamera le paiement de sa facture.



Dans le cas de la fraude au Président, le fraudeur se fait passer pour le Président de l'entreprise ou pour un tiers (avocat par exemple) et demande le virement de fonds pour une opération confidentielle d'une très grande importance (croissance externe, achat d'une machine …). Il flatte son interlocuteur en lui rappelant la grande confiance que son patron a en lui pour lui parler d'une opération si confidentielle, et il l'intimide en lui indiquant qu'un refus de sa part mettrait en péril l'entreprise… L'emprise psychologique est forte et le collaborateur procède au virement.

COMMENT S'EN PROTEGER ?

1. Sensibiliser les collaborateurs sur ce type d'escroquerie, ils détecteront plus vite la fraude
2. Rappeler aux collaborateurs de l'entreprise d'être vigilant sur l'utilisation des réseaux sociaux, c'est majoritairement sur les réseaux que les fraudeurs récupèrent les informations
3. Mettre en place des procédures de contrôle interne en renforçant les étapes de validation à partir d'un certain seuil ou pour les opérations internationales (Système de double validation par exemple)
4. Vérifier l'authenticité des coordonnées bancaires des clients / fournisseurs avant d'effectuer une opération et se méfier des changements de RIB en dernière minute
5. Demander des précisions sur l'interlocuteur et penser à vérifier le numéro de votre interlocuteur habituel et éventuellement passer un contre appel

ET EN CAS D'ATTAQUE ?

- Prendre contact rapidement avec sa banque et demander le retour des fonds
- Déposer une plainte auprès des services et gendarmerie

N'hésitez pas à contacter votre interlocuteur du Groupe PTBG si vous souhaiter vous faire accompagner sur le sujet.

LE CHEQUE NUMERIQUE

AIDE A LA NUMERISATION DE 500 €

Vous êtes éligibles si :

- vous êtes une personne physique ou une entreprise inscrite au répertoire des métiers ou au registre du commerce et des sociétés
- vous respectez des critères de taille (chiffre d'affaires ou bilan inférieur à 2M€, effectif inférieur à 11 salariés)
- vous avez subi une interdiction d'accueil du public à compter du 30 octobre 2020

Les dépenses prises en comptes doivent :

- Etre d'un montant minimal de 450€
- Être datés entre le 30 octobre 2020 et le 31 mars 2021 inclus
- Correspondre à un achat ou un abonnement de solution numériques ou un accompagnement à la numérisation
- Relever des thèmes suivants : e-commerce, paiement en ligne, outil de cybersécurité, stockage de données, outil de gestion des relations clients …

La demande d'aide est à adresser avant le 28 mai 2021 pour les factures datées avant le 28 janvier 2021 et dans les 4 mois de la facture pour celles datées après.

Nous contacter

COMMENT ALLIER TRAVAIL À DISTANCE ET SÉCURITÉ DES DONNÉES ?

92% en 2017, **80%** en 2018, **65%** en 2019… Si le nombre d'entreprises françaises subissant une ou plusieurs cyberattaques diminuent d'année en année, c'est parce qu'elles investissent dans la cybersécurité.

Mais cette réalité est tout autre en télétravail où les salariés ne disposent pas toujours des mêmes outils pour se protéger des hackers. La preuve : 30 % des professionnels de la sécurité affirment qu'il y a eu une augmentation des incidents de sécurité contre leur organisation suite à la mise en œuvre du travail à distance, selon une enquête de l'International Information System Security Certification Consortium, publiée par **ZDnet.**

En cette période où le télétravail est indispensable pour poursuivre son activité, mais s'annonce aussi comme une méthode de collaboration durable, il est temps de se poser cette question : comment allier travail à distance et sécurité des données ?

PREMIERE REGLE : DES SALARIES BIEN EQUIPES

En télétravail, les salariés travaillent souvent avec leurs propres ordinateurs, sur un réseau Wi-Fi pas forcément sécurisé. Ce qui offre une brèche aux potentielles attaques.

La meilleure solution ? Donner les moyens au télétravailleur de se protéger. Vous devez lui fournir des équipements appropriés et sécurisés. À la place de l'ordinateur personnel, les salariés en télétravail peuvent travailler depuis un PC fourni par l'entreprise, qui dispose d'un accès au réseau informatique, ainsi qu'aux pares-feux professionnels.

Pensez aussi à leur fournir un smartphone : les téléphones portables aussi peuvent être source de failles exploitables pour les cybercriminels !

UNE CONFIGURATION OPTIMALE DES SERVICES DE BUREAU A DISTANCE

Même s'ils fluidifient les échanges entre télétravailleur et entreprise, les services de bureau à distance possèdent une certaine vulnérabilité. Dès qu'un outil communique avec l'extérieur, il devient sensible aux attaques. Le bureau à distance n'échappe pas à la règle et les pirates informatiques peuvent y accéder pour contrôler le fonctionnement de votre infrastructure.

Pour vous protéger :

- Autorisez uniquement l'accès aux adresses IP provenant du serveur VPN de votre entreprise.
- Utilisez des mots de passe complexes pour accéder au bureau à distance.
- Activez l'authentification multi-facteur (MFA) pour les télétravailleurs.
- Établissez une liste blanche des adresses IP fournies par les salariés en télétravail.
- Assurez-vous de vérifier régulièrement les journaux d'accès à votre serveur pour déceler des connexions suspectes (et y remédier immédiatement)
- Mettez à jour vos services de bureau à distance à chaque update.

UNE POLITIQUE DE MOTS DE PASSE RENFORCEE, COMME TOUJOURS !

En travaillant à domicile, la tentation d'utiliser des mots de passe simple, faciles à retenir et uniques est grande. Même si cette méthode simplifie la vie du salarié, cela fragilise **la sécurité des données de l'entreprise.**

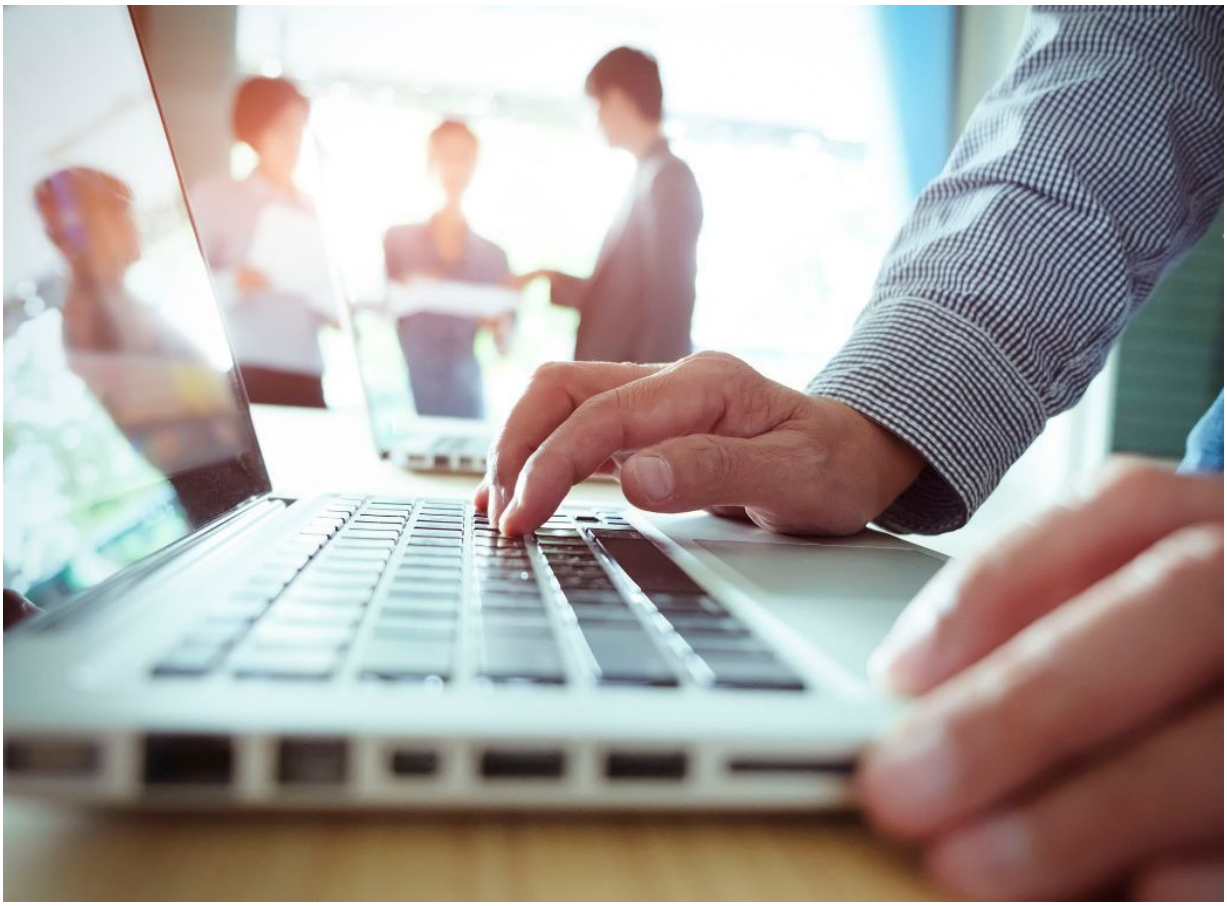
Le télétravailleur doit opter pour des mots de passe suffisamment longs, complexes et pas toujours en lien avec sa vie personnelle. Configurez vos outils et applications pour qu'ils obligent

les utilisateurs à utiliser des chiffres, des caractères spéciaux et des majuscules. Implémentez également une double authentification, notamment si un nouveau périphérique tente de se connecter au système d'information de votre entreprise.

Par ailleurs, vos collaborateurs devraient éviter d'utiliser un mot de passe unique pour tous les périphériques et services. Si cette technique facilite la gestion, elle est risquée : à la moindre faille, le cybercriminel peut accéder à l'ensemble de vos données !

Pensez à implémenter des solutions pour contrecarrer des attaques par force brute qui aident à casser un mot de passe en quelques secondes.

Enfin, dans le cadre du travail à distance, il convient de définir un renouvellement des mots de passe plus fréquent (tous les 30 jours, par exemple).



GARDER UN ŒIL SUR LA JOURNALISATION

Si, malgré toutes les précautions, vous avez subi une attaque, vous devez permettre à **vos experts informatique** d'analyser l'incident. Cela passe par la journalisation.

En effet, ce système récolte et archive les activités menées sur le réseau. Si un pirate arrive à investir votre informatique, il va forcément laisser des traces de son passage.

S'il est trop tard pour empêcher les dégâts à l'instant T, la journalisation permet de détecter les failles et de les combler. Elle vous aide à anticiper les prochaines attaques.

Pour ce faire :

- Activez la journalisation sur les équipements des télétravailleurs et des services exposés.
- Envoyez les données vers une plateforme de gestion des informations et des événements de sécurité (SIEM).

Le télétravail expose un peu plus les données de votre entreprise aux attaques. Donner les moyens à vos salariés de se protéger demeure la première règle en cybersécurité.

Cependant, n'omettez pas de prendre aussi les mesures en interne grâce à une régularisation des accès à distance, un renforcement de vos dispositifs de sécurisation et une surveillance constante des activités menées sur votre réseau informatique.

Nous contacter

ALTICAP
LA PRODUCTIVITÉ DONNE DES AILES

GROUPE PLB
Raisons de plus

ALTICAP
LA PRODUCTIVITÉ DONNE DES AILES

EM NORMANDIE
MÉTIS LAB