



Situation

Réponses :

- ▶ Cette demande semble légitime et le mail personnalisé met en confiance
- ▶ La mention "pour éviter les litiges" revêt un caractère stressant pour le collaborateur
- ▶ Un changement de RIB peut avoir des conséquences financières importantes si l'une des sociétés a été piratée

Situation

Miguel reçoit le nouveau RIB d'un fournisseur

Boîte de réception



De: 1sifon - comptabilité
<services-finance@1sifon >

À: Miguel@masociete.com

Sujet: Service Comptabilité

Cher Miguel,

Nous vous signalons des modifications apportées
à nos données bancaires.

Pour éviter les litiges, veuillez en tenir compte
lors du règlement de votre dernière facture en
utilisant nos nouvelles coordonnées bancaires
(RIB) que vous trouverez en pièce jointe.

Bien cordialement,
Service Comptabilité



1pièce jointe: RIB_nouveau_1sifon.pdf



Situation

Réponses :

- ◀ L'adresse du site est suspecte
- ◀ Le message est anxiogène et la procédure d'installation n'est pas habituelle (hors magasin d'application)
- ◀ Le message système (en bas) renforce la suspicion de danger en cas d'installation

Situation

Redouane vient de cliquer sur un lien contenu dans un mail. Soudain, une fenêtre apparaît





Situation

Réponses :

- ▶ L'adresse mail de l'émetteur est suspecte car elle ne provient pas de la société
- ▶ Le risque de blocage de messagerie est un argument stressant pour Natasha
- ▶ Le ton du courriel est directif et la signature de la "Direction" suggère un ordre hiérarchique
- ▶ Le lien "authentification" est suspect

Situation

Natasha reçoit un mail du service informatique

Boîte de réception



De: Support informatique
< masociete.secure@radiopwn.com >

À: Natasha@masociete.com

Sujet: NOTIFICATION ALERTE DE VOTRE
MESSAGERIE // ACTION REQUISE

Suite à une mise à jour de nos services, des travaux sont effectués sur le serveur de notre messagerie.

Pour éviter que votre compte soit suspendu, veuillez confirmer l'utilisation de votre adresse e-mail.

Pour cela, Cliquez sur: AUTHENTIFICATION pour effectuer la mise à jour.

Nous nous excusons pour le désagrément.

La Direction

AUTHENTIFICATION



Situation

Réponses :

- ▶ L'adresse mail de l'émetteur est suspecte car elle ne correspond pas au site officiel malgré sa ressemblance
- ▶ Le message incite au "clic" par curiosité
- ▶ En cliquant sur le bouton "Voir qui vous regarde", on ne sait pas ce qui va se passer

Situation

*Éric reçoit un mail de notification
d'un réseau social*

Boîte de réception



De : recrutement WhosIn
< notifications-noreply@whozz-in.com >
À : Eric@masociete.com
Sujet : [INTERNET] Eric on vous remarque

Whos in



**Votre profil est sous son
meilleur jour**

Votre travail et vos réalisations ne passent
pas inaperçus !

15

vues du profil

Voir qui vous regarde



Situation

Réponses :

- ▶ Serena reçoit des réponses à un message qu'elle n'a pas envoyé
- ▶ Le message reçu par les destinataires mentionne une procédure qui est du domaine du département informatique
- ▶ Certains destinataires n'utilisent même pas la fonctionnalité citée dans le message litigieux

Situation

*Serena reçoit de nombreuses réponses
à un mail qu'elle n'a jamais envoyé*

Courrier entrant



Sujet	Correspondant	Date
Re: Connexion au "share"	Franck	13:37
Re: Tr: Connexion au "share"	Clarissia	12:23
Re: Re: Connexion au "share"	Pavel	11:02
Re: Connexion au "share"	Amandine	10:27

De: Franck@masociete.com

À: Serena@masociete.com

Sujet: Re: Connexion au "share"

← Répondre → Transférer

13:37

Bonjour Serena,

J'ai reçu un mail de ta part avec de nouvelles instructions pour me connecter à notre espace partagé.

Ça me semble bizarre car tu n'en as pas parlé lors de la réunion d'équipe en visio.

Est-ce que cette procédure a été validée par le département informatique ?

Nous sommes plusieurs à avoir reçu ce mail dont certains qui n'utilisent pas le "share".

Bien à toi,

Franck



Situation

Réponses :

- ▶ Le message affiché sur le bureau est alarmant et anxiogène
- ▶ Il indique que l'ensemble des données importantes sont inaccessibles
- ▶ Il donne une consigne vague invitant à ouvrir un fichier, ce qui n'est pas du domaine de l'utilisatrice dans ce contexte

Situation

Yasmine découvre un message sur son ordinateur

DATA LOCK 3.0

**TOUTES VOS DONNÉES IMPORTANTES
SONT VOLÉES ET CHIFFRÉES!**

Vos fichiers ont été volés et chiffrés
pour plus d'information lisez

RESTAUREZ-MES-FICHIERS.TXT

qui est situé dans chaque répertoire chiffré





Situation

Réponses :

- ▶ En utilisant un système non référencé par son entreprise, Asma ne respecte pas la charte "utilisateurs"
- ▶ La confidentialité des données est compromise car aucune assurance n'est donnée quant à la conservation ou la diffusion des fichiers par ce service externe

Situation

Asma envoie des fichiers volumineux au moyen d'un service grand public



https://www.transfert-gratuit.fr



Chargez vos fichiers



Présentation_investisseurs_V4.pptx
Prospects_région_Ouest_v3.pptx

9,8 Mo
5,3 Mo

Envoyer à

miguel@masociete.com

Votre adresse e-mail

asma@masociete.com

Titre

Présentations pour la réunion avec les investisseurs

Message

Si tu as besoin de modifications, fais moi un retour au moins deux jours avant la réunion.

Bonne journée.

Transférer



Situation

Réponses :

- ▶ Laurent a un besoin légitime de se connecter à son réseau d'entreprise
- ▶ Il utilise un réseau gratuit et ouvert au public. Celui-ci est peut-être mal sécurisé ou piraté ou encore son nom peut être usurpé par un WiFi malveillant
- ▶ Rien ne garantit la sécurité de ses échanges qui peuvent être interceptés à moins d'utiliser un VPN

Situation

Laurent est en déplacement professionnel et doit se connecter à son réseau d'entreprise



Gare de Grapencourt

ACCÈS GRATUIT

Entrez votre nom et une adresse e-mail
pour accéder au WiFi

Nom

Laurent

e-mail

laurent@masociete.com

☒ J'accepte les [conditions d'utilisation](#)

CONNECTER

PRO



Situation

Réponses :

Situation

Boîte de réception



De:

À:

Sujet:

PRO



Situation

Réponses :

Situation



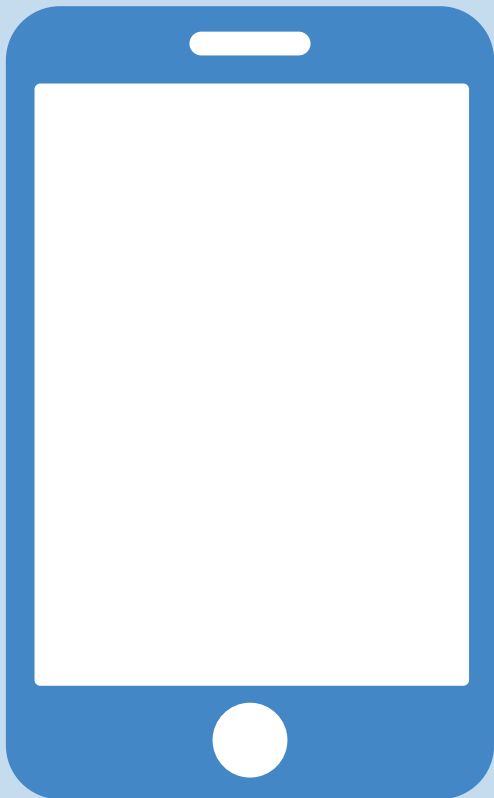
PRO



Situation

Réponses :

Situation



PRO



Situation

Réponses :

Situation

Boîte de réception



De:

À:

Sujet:



1pièce jointe:



Menace

La fraude au virement,
de quoi parle-t-on ?

La **fraude au virement** est une escroquerie reposant sur l'usurpation d'identité d'un responsable ou d'un tiers connu de l'entreprise. Dans certains cas, cette fraude fait suite au piratage et à l'utilisation de la messagerie de la personne ou entité usurpée. Elle peut être facilitée par des recherches sur internet, notamment les réseaux sociaux, qui permettent de connaître les collaborateurs et leurs attributions pour plus de crédibilité.

Fraude au virement (FOVI)

Pourquoi?

Amener la victime à réaliser un virement de fonds sur un compte bancaire détenu par les escrocs (changement de RIB, virement non planifié "urgent et confidentiel").



Comment?

Mail, SMS, courrier ou appel téléphonique d'un escroc qui usurpe l'identité d'un dirigeant, d'un avocat, d'un tiers de confiance, d'un fournisseur, d'un salarié ou d'un client.





Menace

L'hameçonnage,
de quoi parle-t-on ?

L'**hameçonnage** (ou « phishing » en anglais) est le principal mode opératoire des cybercriminels pour dérober des informations professionnelles ou personnelles. En général, il revêt une apparence légitime et crédible, et cherche souvent à provoquer un sentiment d'urgence ou d'intérêt chez les victimes. L'objectif est de les manipuler pour obtenir des informations sensibles ou les rediriger vers des sites internet contrefaits ou malveillants.

Hameçonnage

Pourquoi?

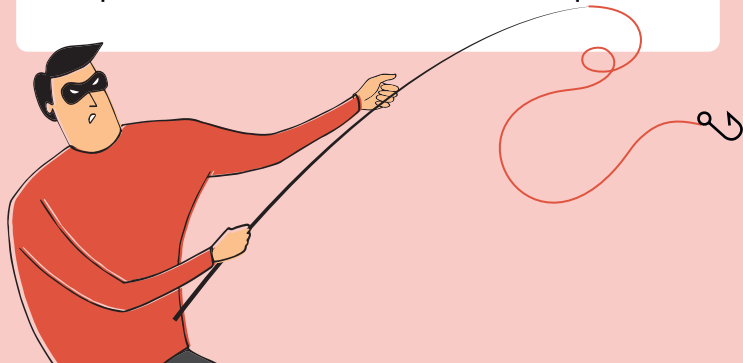


Obtenir des informations confidentielles (identité, adresses, comptes, mots de passe, données bancaires...) pour en faire un usage frauduleux.

Comment?



Courriel, SMS ou appel téléphonique d'un escroc qui se fait passer pour un supérieur hiérarchique, un fournisseur, un prestataire, un client, une banque...





Menace

Le piratage de compte,
de quoi parle-t-on ?

Le **piratage de compte** désigne la prise de contrôle par un individu malveillant d'un compte ou d'un service distant au détriment de son propriétaire légitime.

Il peut s'agir de comptes ou d'applications de messagerie, d'un réseau social, de sites administratifs, d'administration de ressources informatiques internes/externes...

Piratage de compte

Pourquoi?

Se connecter en lieu et place de l'utilisateur légitime pour un usage frauduleux (usurpation d'identité, accès à des échanges/données confidentielles).



Comment?

Prise de contrôle de compte(s) en ligne, en raison d'un mot de passe trop simple, capté par un tiers ou autorisé par erreur/négligence de l'utilisateur.



PRO



Menace

La récupération de données,
de quoi parle-t-on ?

Au sein de chaque entreprise, de nombreuses **données** sont manipulées (salariés, fournisseurs, clients, projets...). Ces données attirent la convoitise des cybercriminels. La responsabilité de l'entreprise et/ou de ses dirigeants peut être engagée en cas de défaut de protection de ces données.

Récupération de données

Pourquoi?

Récupérer des données pour commettre des escroqueries, exercer un chantage ou espionner l'activité de l'entreprise au moyen de ces informations.



Comment?

Service de partage, hébergement ou de conversion de fichiers, point WiFi (...) contrôlé ou usurpé par des pirates.





Menace

Les virus informatiques
de quoi parle-t-on ?

Communément appelés « **virus** », les programmes malveillants ciblent aussi bien les ordinateurs que les téléphones mobiles. Ces programmes malveillants sont généralement contrôlés à distance par les cybercriminels qui les opèrent, parfois dans la durée, pour récupérer des informations ou leur faire déclencher des actions qui servent leurs intérêts.

Virus informatiques

Pourquoi?

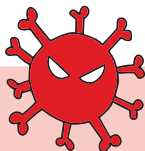


Perturber le fonctionnement d'un appareil ou porter atteinte à ses données: récupération ou altération d'informations (documents, mots de passe, messages); utilisation de l'appareil pour en attaquer d'autres; espionnage.

Comment?



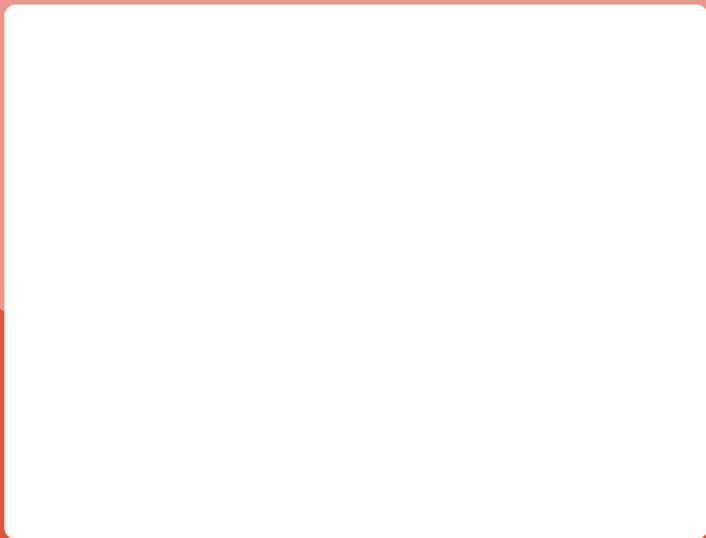
Un appareil peut être infecté par diverses méthodes: en cliquant sur un lien ou une pièce jointe piégé; en naviguant sur un site malveillant ou en téléchargeant un logiciel ou du contenu multimedia piraté.



PRO



Menace



Menace

Pourquoi?

Comment?



Risque

Exemple d'atteinte à l'image :

- Une revendication de piratage est visible sur la page d'accueil d'un site internet. De nombreux internautes la signalent sur les réseaux sociaux et se demandent si leurs données personnelles ont été récupérées par un pirate.
- Une entreprise a été victime d'une fraude au virement pour un montant important. Un escroc a détourné le paiement destiné à son fournisseur. La renommée de la société est mise à mal et le fournisseur va faire un recours judiciaire pour être payé.

Atteinte à l'image

La **réputation** de l'entreprise peut être dégradée suite à des cybermalveillances rendues publiques mettant en avant un défaut de sécurité ou de professionnalisme (récupération de données, fraude au virement, rançongiciel...).

Cette mauvaise publicité peut entacher la confiance des clients, fournisseurs ou partenaires.





Risque

Exemple d'escroquerie financière :

- Le service comptabilité reçoit une demande urgente de paiement d'un fournisseur accompagné de son RIB. Cette facture a bien été envoyée via le mail du fournisseur. Malheureusement, il s'est fait pirater sa boîte mail et c'est le cybercriminel qui a fourni ce RIB.
- Un dirigeant reçoit un avis de paiement pour un "affichage obligatoire" "sous peine de sanctions pénales" prérempli avec la fiche de l'entreprise. Cet avis ressemble à une demande officielle mais émane d'une société privée peu scrupuleuse qui a accès au registre du commerce.

Escroquerie financière

L'escroquerie a pour objectif un **gain financier** pour les cybercriminels qui trompent un collaborateur en obtenant de lui des informations, accès, virements en dépit des procédures internes.

Les escrocs peuvent utiliser des ressorts psychologiques comme la crainte, l'urgence, l'empathie ou l'attrait du gain pour piéger leurs victimes.





Risque

Exemples d'indisponibilité du S.I.:

- Le site internet d'une entreprise est hors ligne suite à un afflux massif de connexions malveillantes (« déni de service distribué ») rendant impossible la connexion des clients.
- Le système informatique interne est à l'arrêt suite à un ransomiciel. Il est impossible de communiquer avec les utilisateurs, clients et fournisseurs (mail, téléphonie, applications et données inaccessibles, ordinateurs bloqués...). Les collaborateurs doivent travailler avec les archives papier qui sont incomplètes.

Indisponibilité du système informatique

L'indisponibilité du système d'information est généralement la conséquence du **blocage** des ordinateurs, serveurs ou services de l'entreprise. Il devient alors impossible pour les collaborateurs d'accéder aux fichiers et applications et peut entraîner la mise hors-ligne des services externes pour les clients, fournisseurs ou partenaires.





Risque

Exemples d'usurpation d'identité:

- Un client appelle la société pour une livraison non effectuée.
Après vérifications, il apparaît qu'il a été trompé par un site internet contrefait à partir du site réel de la société.
- En l'absence du PDG, quelqu'un se présentant comme l'avocat de la société appelle le responsable du service comptabilité pour un virement urgent nécessaire à l'obtention d'un contrat important. L'escroc envoie son RIB par mail en usurpant l'identité réelle de l'avocat de la société.

Usurpation d'identité

L'usurpation d'identité est un délit qui désigne l'utilisation d'informations personnelles ou professionnelles permettant d'**identifier une personne ou une organisation sans son accord** pour réaliser des actions frauduleuses.





Risque

Exemples de violation de données :

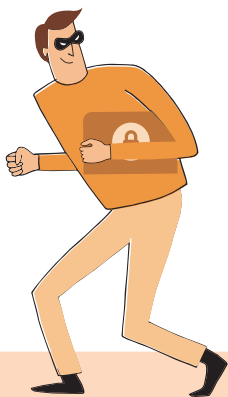
- Un salarié utilise une application pour lire et modifier les fichiers PDF depuis sa clef USB. Cette application a installé discrètement un logiciel qui enregistre toutes les frappes au clavier et les envoie à un cybercriminel.
- Un salarié licencié a conservé ses accès informatiques. Par vengeance, il entreprend d'effacer les données auxquelles il peut encore accéder.
- Après avoir déclaré l'incident à la CNIL, une société avertit ses clients que leurs données ont été exfiltrées par des cybercriminels suite à une attaque par rançongiciel.

Violation de données

La violation de données est la **collecte**, la **modification**, la **destruction** ou la **divulgateion** non autorisée d'informations.

Son origine peut être accidentelle ou malveillante, interne ou externe à l'organisation qui détient ces données.

Elle est souvent la conséquence d'un hameçonnage, d'un piratage, d'une récupération de données ou d'un virus.



PRO



Risque



Risque



PRO



Bonne pratique



Assistance et prévention
en cybersécurité



Limitez la publication d'informations concernant votre société/organisation et ne publiez pas d'informations internes sensibles **sur internet et les réseaux sociaux** (dénomination de poste, projets, structure de la société, fournisseurs...)

PRO



Bonne pratique



Assistance et prévention
en cybersécurité



N'utilisez pas de services externes non validés par l'entreprise pour manipuler des données internes (traduction ou conversion de documents en ligne, transfert de fichiers, outil d'intelligence artificielle...).

Ces données pourraient être utilisées de manière frauduleuse par un tiers.

PRO



Bonne pratique



Assistance et prévention
en cybersécurité



Ne pas divulguer, à l'extérieur ou à un contact inconnu, par mail ou téléphone, **des informations sur le fonctionnement de la société**, ses fournisseurs et clients (organigramme, contacts, documents comportant la signature d'acteurs-clés, procédures internes...).

PRO



Bonne pratique



Assistance et prévention
en cybersécurité



En cas de demande de virement ou de changement de coordonnées bancaires (fournisseur, employé, avocat...) reçue par message ou appel, **vérifiez systématiquement** l'identité de votre correspondant en l'appelant directement à un numéro de téléphone en votre possession.

PRO



Bonne pratique



Assistance et prévention
en cybersécurité



Ne désactivez jamais l'antivirus installé par votre organisation sur vos appareils (ordinateur, téléphone, mobile, tablette).

N'installez pas d'applications ou de programmes autres que ceux validés par l'entreprise.

Des logiciels dont l'origine ou la réputation sont douteuses peuvent contenir des virus.

PRO



Bonne pratique



Assistance et prévention
en cybersécurité



Signalez toute sollicitation suspecte à vos collègues, responsables ou support technique qu'il s'agisse :

- d'un appel ou mail suspect,
- d'un changement de coordonnées bancaires (RIB),
- d'une demande de virement non planifiée.

Cela peut permettre de mettre au grand jour une attaque ciblée contre votre organisation.

PRO



Bonne pratique



Assistance et prévention
en cybersécurité



Soyez vigilant avec les liens ou les pièces jointes contenus dans les mails, SMS ou QRcode qui peuvent vous mener vers une page d'hameçonnage (phishing) ou infecter votre appareil.

Vérifiez bien l'adresse du site avant de renseigner des données.

En cas de doute, saisissez directement dans votre navigateur l'adresse du site concerné.

PRO



Bonne pratique



Assistance et prévention
en cybersécurité



Utilisez des mots de passes différents et complexes pour chaque site et application. Vous pouvez utiliser un **gestionnaire de mots de passe** pour les stocker.

Activez la double authentification lorsque les sites ou les services le permettent, pour augmenter le niveau de sécurité de vos comptes.

PRO



Bonne pratique



Assistance et prévention
en cybersécurité



En mobilité ou télétravail, utilisez le VPN (réseau privé virtuel) de l'entreprise pour vous connecter à son système informatique.

Privilégiez la connexion au réseau téléphonique (4G/5G) plutôt qu'à un WiFi Public (hôtels, gares...). Ces réseaux WiFi, souvent mal sécurisés, peuvent être contrôlés ou usurpés par des pirates qui pourraient capter vos données.

PRO



Bonne pratique



Assistance et prévention
en cybersécurité



Faites les mises à jour de vos appareils, applications et logiciels dès qu'elles sont proposées pour corriger leurs failles de sécurité qui peuvent être utilisées par des cybercriminels.

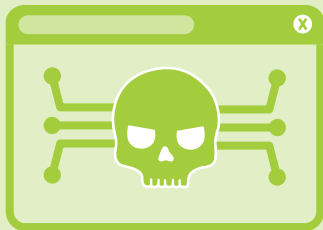
PRO



Bonne pratique



Assistance et prévention
en cybersécurité



En cas d'infection réelle ou supposée d'un équipement, **il faut le déconnecter d'internet et du réseau** d'entreprise pour éviter la contamination d'autres équipements (déconnecter le WiFi, débrancher le câble réseau).

Ne pas éteindre l'appareil et contacter immédiatement votre support, prestataire ou référent informatique car des éléments techniques peuvent parfois être récupérés.

PRO



Bonne pratique



Assistance et prévention
en cybersécurité



Connaître et respecter la charte informatique interne.

Ce document établit les droits et obligations des collaborateurs dans les usages numériques au sein de son organisation.

En cas de manquement, votre responsabilité personnelle pourrait être engagée.

PRO



Bonne pratique



Assistance et prévention
en cybersécurité



N'utilisez pas des services grand public à des fins professionnelles pour le stockage de données et les courriels (cloud, transfert de fichiers, transfert de mail vers une adresse personnelle...).

Les outils professionnels disposent souvent de protections supplémentaires permettant de limiter les fuites de données.

PRO



Bonne pratique



Assistance et prévention
en cybersécurité



Ne connectez pas de matériels personnels ou publicitaires sur des ordinateurs professionnels.

Les supports de stockage externes personnels peuvent contenir des virus (clef usb, disque dur...).

Connecter un téléphone mobile à un ordinateur pour le recharger via USB peut compromettre sa sécurité en diffusant un virus préalablement présent sur le mobile. Cela revient à brancher une clef USB.

PRO



Bonne pratique



Assistance et prévention
en cybersécurité



Sauvegardez régulièrement vos données (sur un disque dur externe, clef USB, serveur, cloud...) et **testez leur restauration** pour pouvoir les retrouver en cas de panne, perte, vol, destruction ou piratage de vos appareils.

Déconnectez systématiquement le support de sauvegarde après utilisation.

PRO

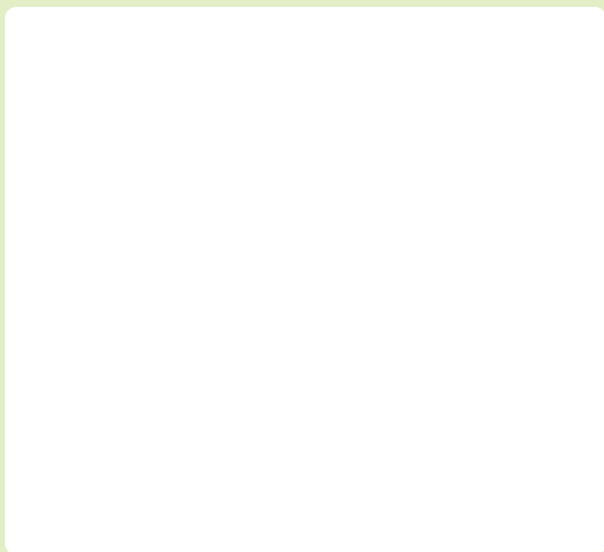


Bonne pratique



Assistance et prévention
en cybersécurité

Bonne pratique



Situation

- (1) *Natasha reçoit un mail du service informatique*
- (2) *Éric reçoit un mail de notification d'un réseau social*
- (3) *Laurent est en déplacement professionnel et doit se connecter à son réseau d'entreprise*
- (4) *Asma envoie des fichiers volumineux au moyen d'un service grand public*
- (5) *Miguel reçoit le nouveau RIB d'un fournisseur*
- (6) *Serena reçoit de nombreuses réponses à un mail qu'elle n'a jamais envoyé*
- (7) *Yasmine découvre un message sur son ordinateur*
- (8) *Redouane vient de cliquer sur un lien contenu dans un mail. Soudain, une fenêtre apparaît*

Menace

**Hameçonnage
(phishing)**

**Récupération
de données**

**Fraude au
virement**

**Piratage de
compte**

**Virus
informatique**

