LES ARNAQUES FINANCIÈRES ET LES CYBER-MENACES:

ENJEU STRATEGIQUE DES ENTREPRISES

BANQUE DE FRANCE
EUROSYSTÈME

EDUCFI
Éducation économique budgétaire et financière

QUIZ

Qu’est-ce qu’un F.O.V.I ?

A – Une arnaque par usurpation destinée à provoquer un virement frauduleux.

B – Le nom d’un fournisseur d’internet.

C – Le nom d’un logiciel de rangement.

QUIZ

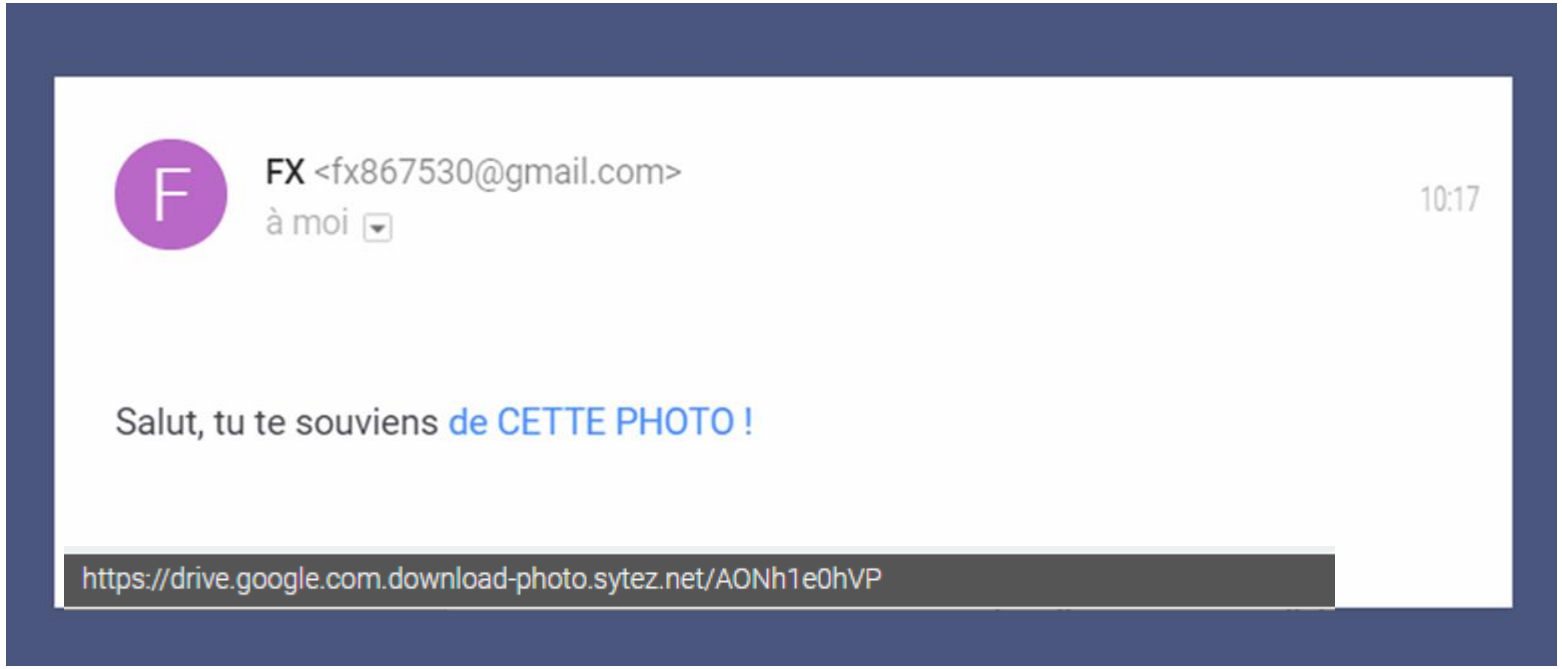
Qu’est-ce qu’un F.O.V.I ?

A – Une arnaque par usurpation destinée à provoquer un virement frauduleux.

B – Le nom d’un fournisseur d’internet.

C – Le nom d’un logiciel de rangement.

QUIZ

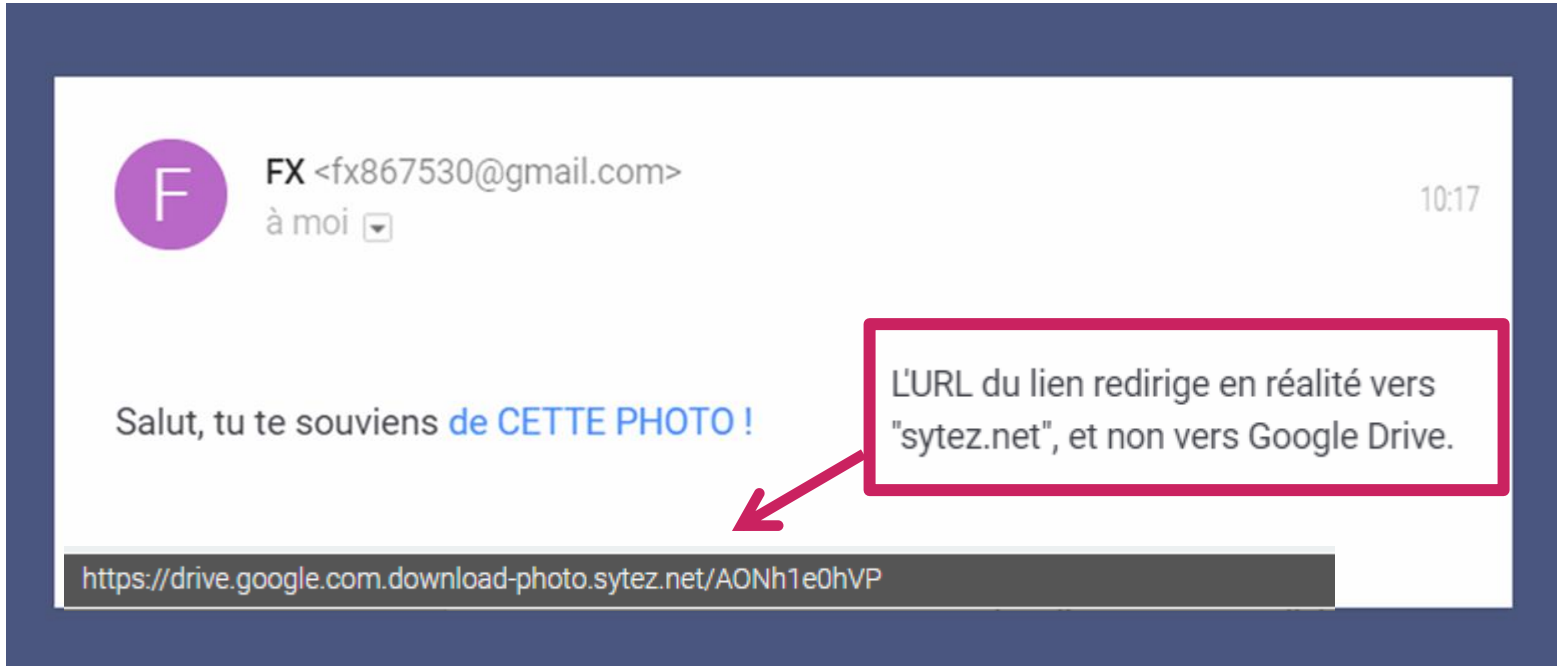


S’agit-il d’un mail frauduleux ?

A – Oui.

B – Non.

QUIZ



S'agit-il d'un mail frauduleux ?

A – Oui.

B – Non.

QUIZ

Quel est le mot de passe le plus robuste ?

A –123456.

B – Ma!Colloc412.

C – Votre date de naissance.

QUIZ

Quel est le mot de passe le plus robuste ?

A –123456.

B – Ma!Colloc412.

C – Votre date de naissance.

QUIZ

Une attaque DDoS qu’est-ce que c’est ?

A – Une attaque de grande ampleur visant à saturer le trafic.

B – Une attaque sur les dossiers du répertoire.

C – Une attaque d’un réseau social.

QUIZ

Une attaque DDoS qu’est-ce que c’est ?

A – Une attaque de grande ampleur visant à saturer le trafic.

B – Une attaque sur les dossiers du répertoire.

C – Une attaque d’un réseau social.

SOMMAIRE

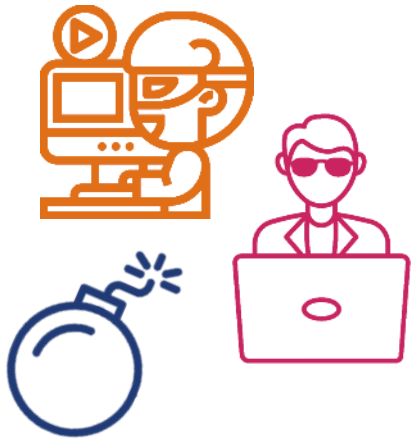
1 SAVOIR IDENTIFIER

2 SAVOIR SE PROTÉGER

3 SAVOIR RÉAGIR

BANQUE DE FRANCE
EUROSYSTÈME

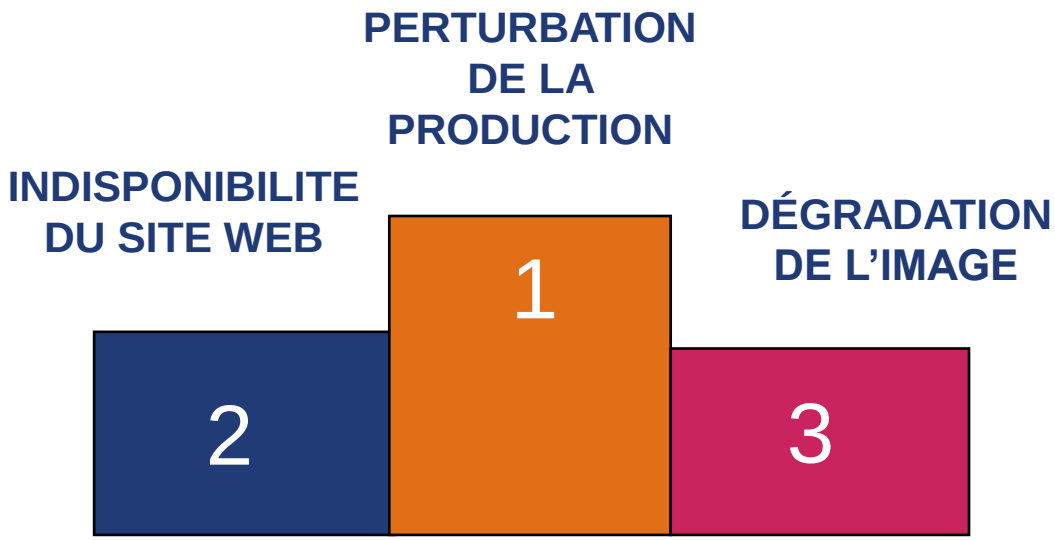
EDUCFI
Éducation économique budgétaire et financière



1

SAVOIR IDENTIFIER

LA CYBERCRIMINALITÉ ET LES ARNAQUES : QUELLES CONSÉQUENCES POUR L'ENTREPRISE ?



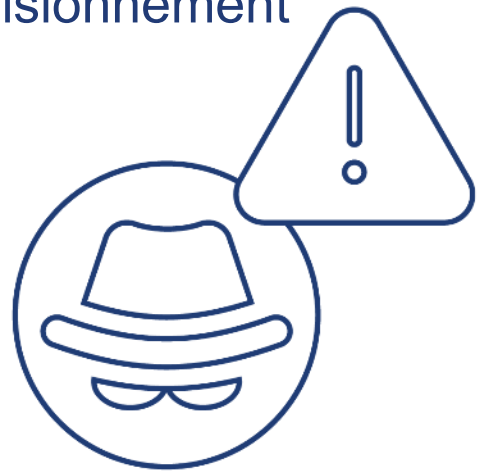
1. **Des conséquences financières à court-terme :** interruption du fonctionnement de l'entreprise, coûts générés par la réponse à l'attaque, perte de matériel informatique.

2. **Des conséquences réputationnelles sur le long-terme :** atteinte à la notoriété de l'entreprise, perte de compétitivité, perte de clients/fournisseurs, effet éventuel sur les effectifs.

LES PRINCIPALES TECHNIQUES

- **Attaque en déni de service (DDoS)**
- **F.O.V.I. :** arnaque au faux président, au faux fournisseur…
- **Attaque par mot de passe**
- **Rançongiciel**
- **Piratage de systèmes informatiques et intrusions**
- **Virus informatiques** (malwares)
- **Hameçonnage**

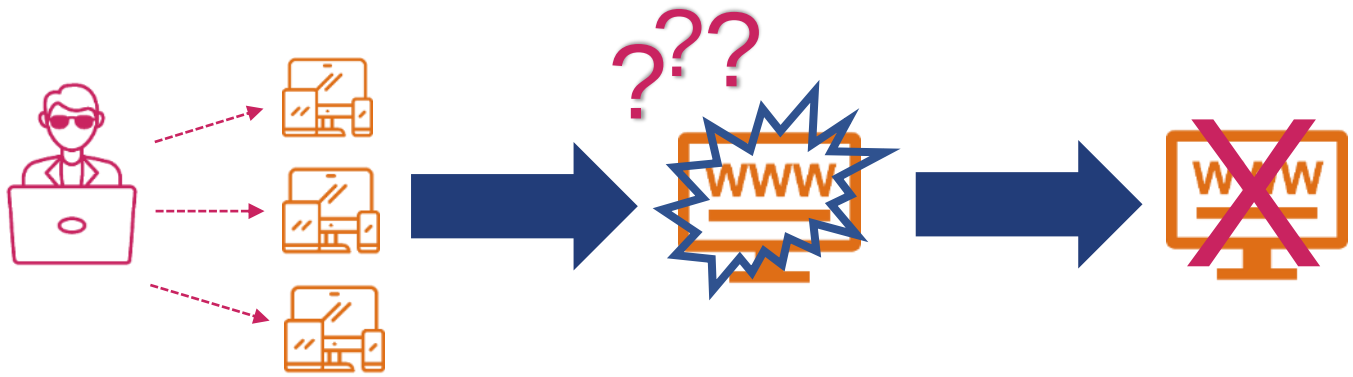
Mais aussi : défiguration de site internet, attaque de la chaîne d'approvisionnement chantage à l'ordinateur prétendument piraté, fausse offre d'emploi…



→ **Le plus souvent, les assaillants combinent différentes formes d'attaques pour multiplier leurs chances de succès et leurs impacts**

Source : Big Media, Bpifrance (2025)

LES ATTAQUES CONTRE LA PRÉSENCE DIGITALE DE L'ENTREPRISE : « DÉNIS DE SERVICE »



- **Principe :** génération d'un trafic démesuré sur le site ciblé afin de générer un nombre de requêtes trop important saturant le service, afin de le rendre inaccessible.
- **Conséquences :** ralentissement du système, accès interrompu aux produits ou aux services, en interne ou en externe.
- **Objectifs :** nuire à la présence en ligne de l'entreprise, pour dégrader son image ou interrompre son fonctionnement – avec éventuellement la demande d'une rançon.

LE PIRATAGE INFORMATIQUE : INTRUSION ET PRISE DE CONTRÔLE DU SYSTÈME INFORMATIQUE

Cette catégorie d'attaques vise à pénétrer le système informatique de l'entreprise – soit à des fins d'**espionnage**, soit pour en **prendre le contrôle** – et parfois pour ces deux motifs !
Elles reposent souvent sur les mêmes vecteurs : **virus**, **attaque de mots de passe**, **hameçonnage**…

ESPIONNAGE :

Objectifs : collecte de données sensibles, vol de secrets industriels, attaque des partenaires de l'entreprise, chantage a posteriori

Types d'attaques : spyware, attaque de la chaîne d'approvisionnement…

PRISE DE CONTRÔLE :

Objectifs : chantage, virements frauduleux, dégradation de l'image de l'entreprise

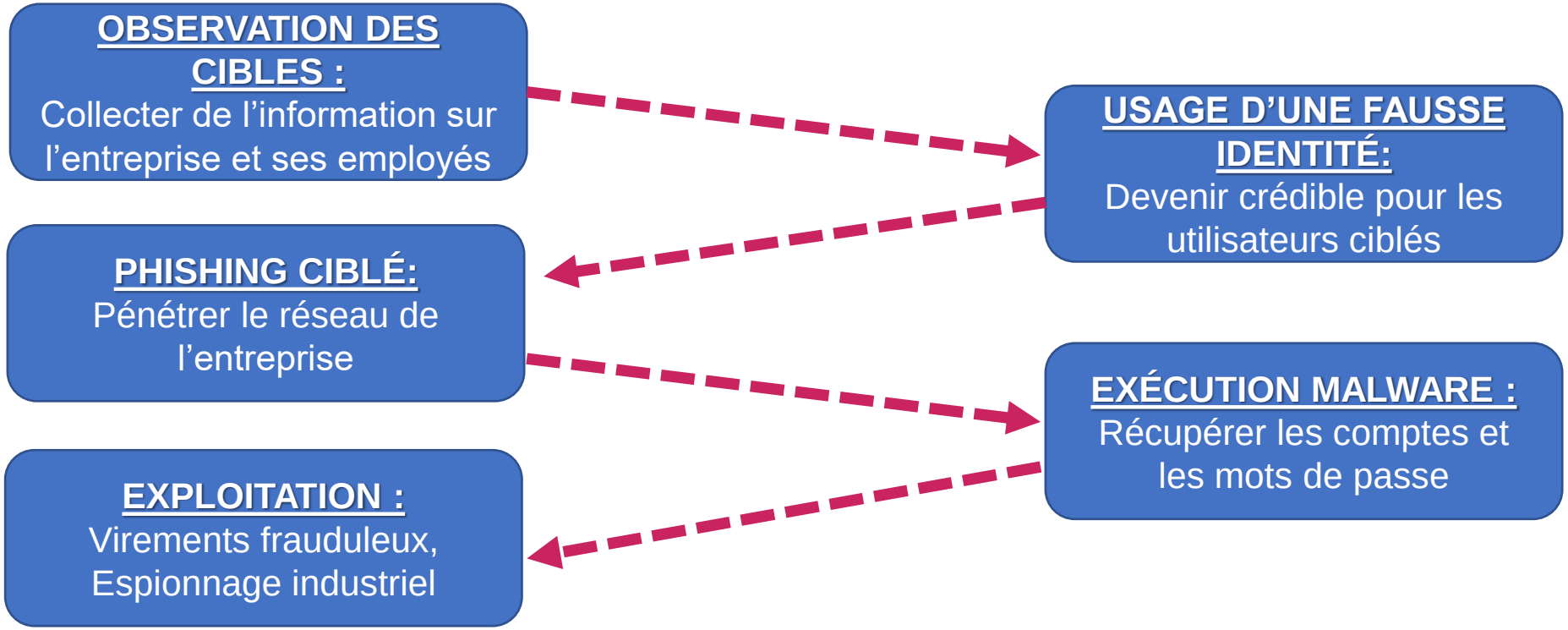
Types d'attaques : rançongiciels, piratage de compte…

Le piratage de compte peut utiliser comme vecteur la technique du hameçonnage, ou « **PHISHING** », consistant à leurrer la victime en l'incitant à remplir un faux formulaire ou à cliquer sur un lien pour récupérer les informations d'accès et de connexion.

LES FAUSSES IDENTITÉS ET LES MÉTHODES D'INGÉNIERIE SOCIALE :

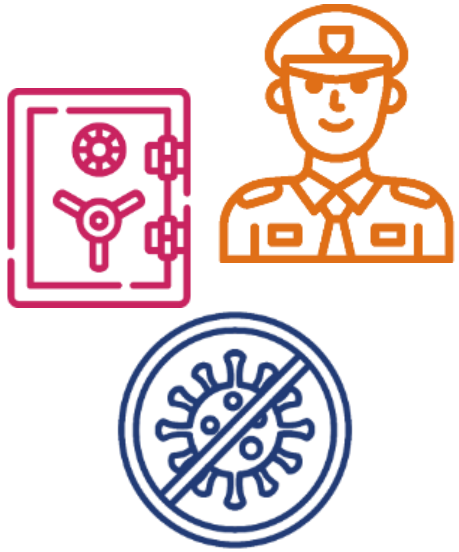
De nombreuses attaques vont reposer avant tout sur la manipulation, plutôt que sur des outils techniques sophistiqués. Elles supposent souvent l'usage d'une fausse identité afin de tromper la cible.

- **Exemple de déroulé d'une attaque reposant sur l'ingénierie sociale :**



Exemples : Faux ordre de virement (arnaque au président), Fausse offre d'emploi…

C'est parfois l'identité de l'entreprise elle-même qui est usurpée : des cybercriminels se font passer pour l'entreprise à son détriment.



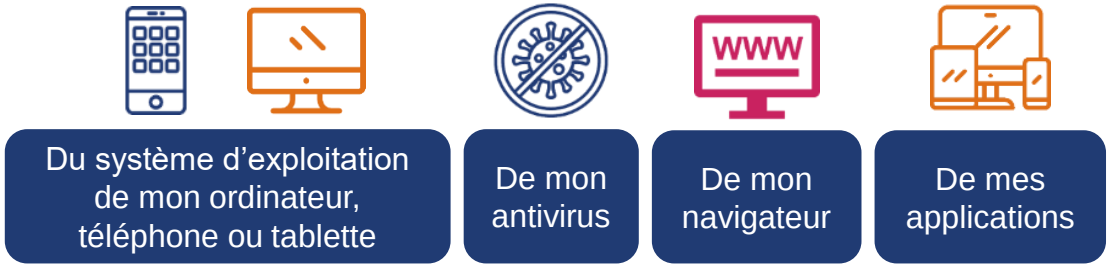
2

SAVOIR SE PROTÉGER

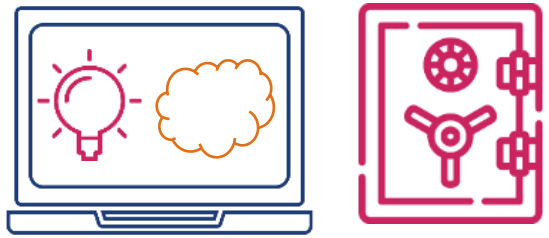
BANQUE DE FRANCE
EUROSYSTÈME
EDUCFI
Éducation économique budgétaire et financière

L'HYGIÈNE NUMÉRIQUE : PRÉSERVER SON SYSTÈME INFORMATIQUE DES VIRUS

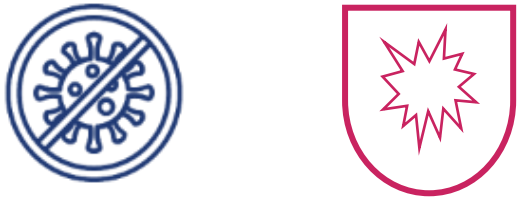
Je m'assure de la **mise à jour régulière** :



J'effectue des **sauvegardes** :



Je protège **ma navigation** :



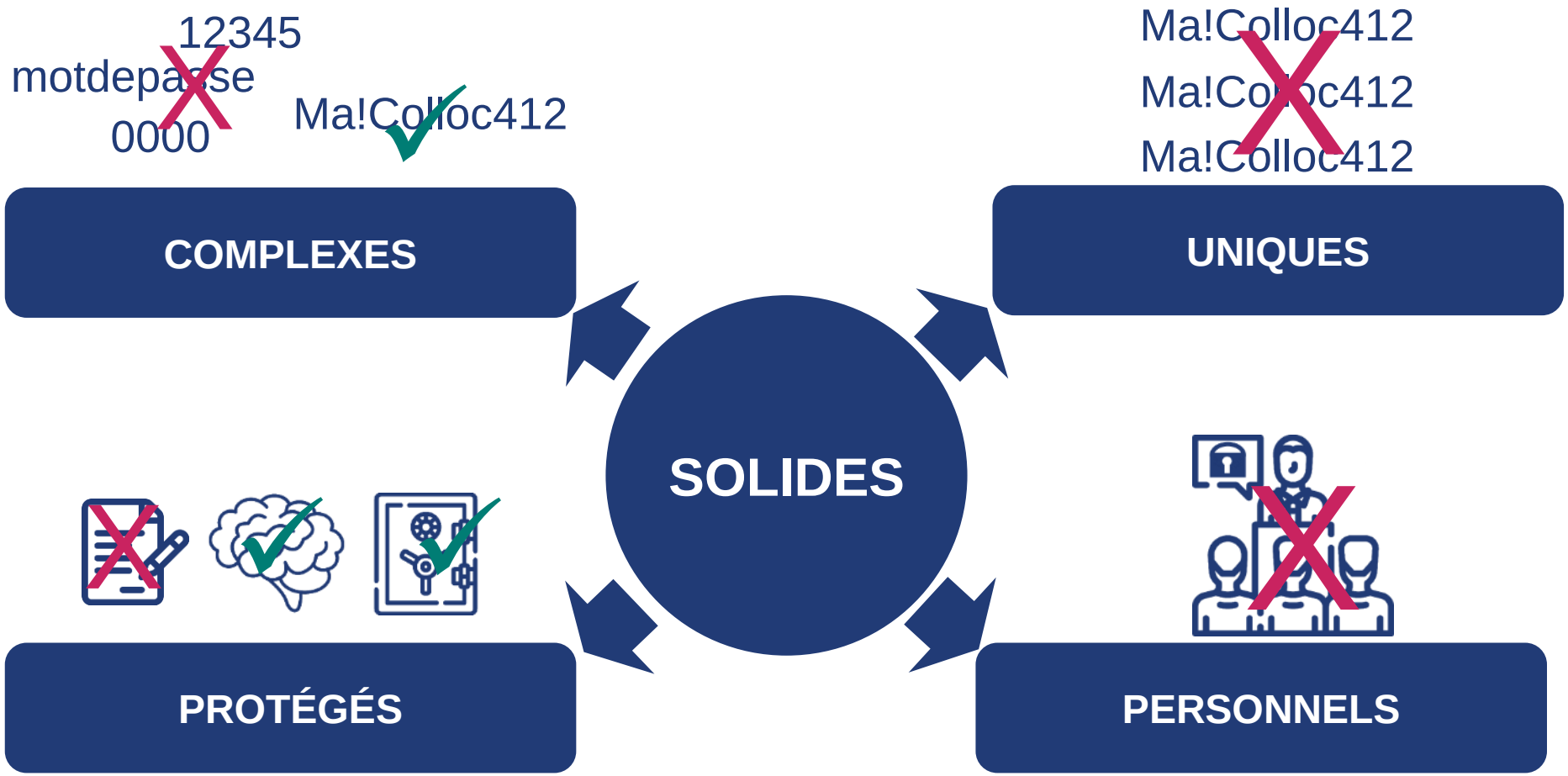
ANTIVIRUS **PARE-FEU**

Je suis vigilant **en déplacement** :

Je me méfie des wifi publics !

DES MOTS DE PASSE SOLIDES POUR SE PROTÉGER DU PIRATAGE

Et plus globalement pour tous vos accès / comptes en ligne !



APPRENDRE À DÉJOUER LE PHISHING : LES BONS RÉFLEXES

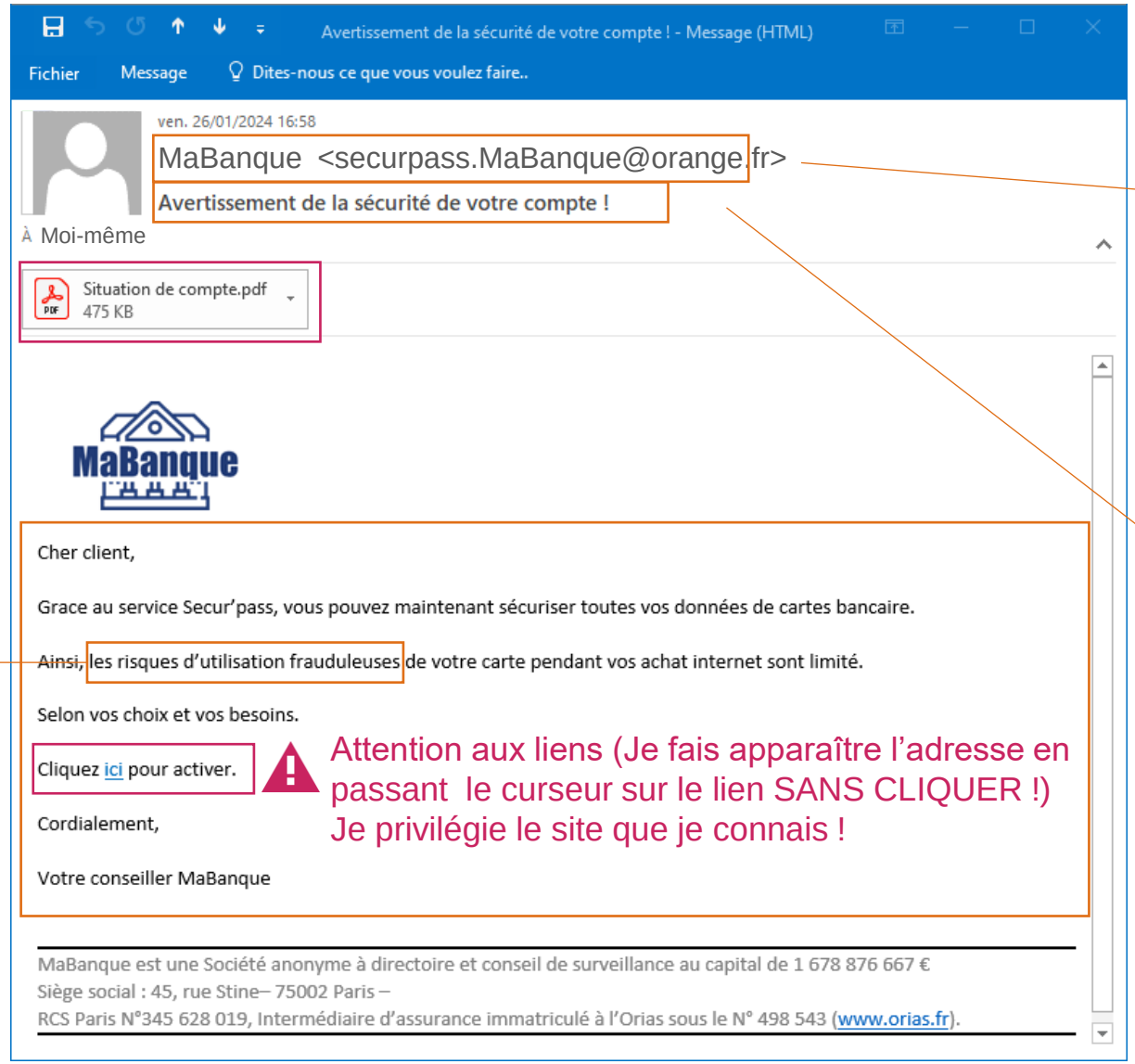
- **Observez bien** l'email, l'adresse de réponse, celle des liens présents …
- **Évitez de cliquer sur des liens** provenant de sources inconnues (préférer aller sur les sites internet directement par leur adresse URL).
- **Redoublez de vigilance** si le mail vous invite à cliquer sur un lien en adoptant un **ton anxiogène** ou à l'inverse **excessivement promotionnel** pour vous faire réagir en urgence.
- **Faire des campagnes de sensibilisation** régulières aux employés.

Le risque de phishing concerne les mails et spams mais aussi les SMS et les réseaux sociaux !

APPRENDRE À DÉJOUER LE PHISHING : CAS PRATIQUE

Attention aux pièces jointes

On cherche souvent à faire peur, à invoquer l'urgence, bref… à m'empêcher de réfléchir !



Attention aux liens (Je fais apparaître l'adresse en passant le curseur sur le lien SANS CLIQUER !) Je privilégie le site que je connais !

Attention à l'adresse mail !

Même s'il n'y a pas de fautes, le niveau de langage du mail peut m'alerter

DÉJOUER L'INGÉNIERIE SOCIALE : SE MÉFIER DES RESSORTS PSYCHOLOGIQUES

- Un escroc peut effectuer des recherches sur **les moteurs de recherche**, sur **les réseaux sociaux** puis prendre contact avec vous. Il vous incitera **à dévoiler des informations** qu'il exploitera ensuite : mots de passe, données personnelles etc. Il peut également obtenir des informations à l'occasion d'**un simple appel téléphonique**.

- Certains ressorts psychologiques bien connus des cybercriminels augmentent leurs chances de succès, et les repérer dans leurs discours peut vous permettre de déjouer une attaque :
  - Sentiment d'**urgence**
  - Appât du **gain**
  - Recours à la menace ou à l'**autorité**
  - **Ressorts émotionnels** (sympathie, pitié…)

DÉJOUER L'INGÉNIERIE SOCIALE : IDENTIFIER LES USURPATIONS D'IDENTITÉ ET LES FAUX SITES

Comment s'assurer de l'authenticité d'un client / fournisseur/ partenaire d'affaire ?

10 éléments à vérifier :

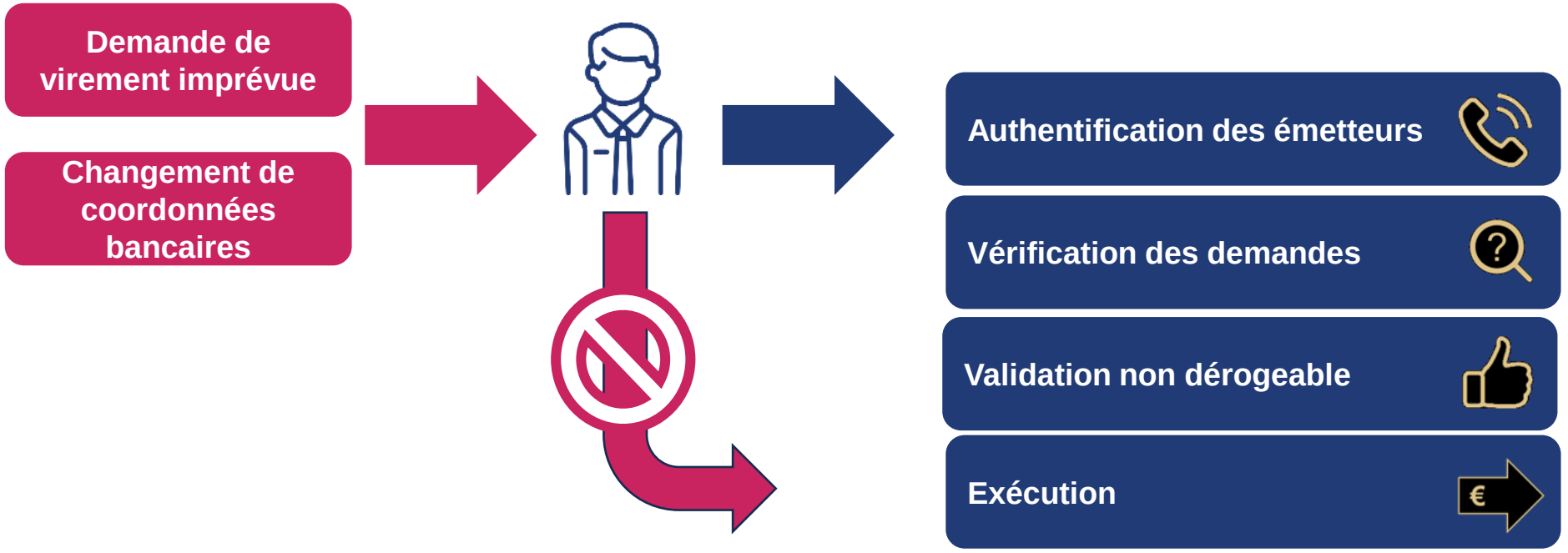
- Interroger le registre national des sociétés
- Vérifier la date d'enregistrement du site web et de son propriétaire
- Vérifier les adresses mails et numéros de téléphone par contre-appels
- Consulter l'adresse physique
- Analyser la présence en ligne de l'entreprise
- Observer les textes du site web
- Vérifier les mentions légales
- S'intéresser au logo
- S'intéresser aux témoignages clients
- S'intéresser à la légitimité du site

Source : francenum.gouv.fr

DÉJOUER L'INGÉNIERIE SOCIALE : LES BONNES PRATIQUES FACE AUX FOVI

Votre personnel doit **être systématiquement formé à ce type de risques** et vérifier avec un appel en cas de doute. Parmi les autres bons gestes :

- **Définition d'une procédure spécifique et non dérogeable d'intégration des IBAN** avec vérification préalable
- **Limitation des informations accessibles permettant l'identification des collaborateurs habilités à gérer les virements** par un acteur extérieur
- **Vérification de l'authenticité des nouveaux partenaires de l'entreprise**, et en particulier de leurs informations bancaires.



PILOTER SA CYBERSÉCURITÉ EN 10 RÈGLES

ÉVALUER SON NIVEAU DE PROTECTION

1. Faire un état de lieux de ses actifs numériques
2. Évaluer le risque
3. Évaluer le niveau de protection actuelle
4. Définir un plan d'action
5. Se faire accompagner

PRÉPARER SES ÉQUIPES

1. Sensibiliser ses collaborateurs
2. Se préparer au pire
3. S'impliquer

CONTRÔLER SA PROTECTION DANS LE TEMPS

1. Contrôler les mesures mises en place
2. Réviser tous les 2 à 3 ans sa stratégie de protection

Source : cybermalveillance.gouv.fr

3

SAVOIR RÉAGIR

BANQUE DE FRANCE
EUROSYSTÈME

EDUCFI
Éducation économique budgétaire et financière

QUE FAIRE EN CAS D'ATTAQUE DDOS ?

1. **S'assurer du diagnostic :** un site peut être inaccessible pour d'autres raisons, et l'entreprise peut ainsi contacte son hébergeur afin de vérifier l'absence de souci technique et la faille éventuelle.

2. **Ne pas payer la rançon éventuellement réclamée.**

3. **Déposer plainte auprès du commissariat.**

4. **S'assurer que son hébergeur est paré pour faire face à la réitération de ce type d'attaques.**

COMMENT RÉAGIR FACE À UNE CYBERATTAQUE VISANT LE SYSTÈME INFORMATIQUE

La clé : réagir rapidement.

Les réflexes face à la crise :

- Alerter le support informatique
- Déconnecter la machine d'internet ou du réseau informatique
- Constituer une équipe de gestion de crise
- Consigner les actions entreprises
- Conserver ou faire conserver les preuves par un professionnel

Piloter la crise :

- Mettre en place les systèmes de secours permettant un service minimal
- Alerter sa banque
- Prévenir son assureur
- Porter plainte
- Notifier l'incident à la CNIL
- Prévenir ses partenaires
- Ne pas payer la rançon
- Reprise progressive et contrôlée

Source : cybermalveillance.gouv.fr

COMMENT RÉAGIR FACE À DES OPÉRATIONS FRAUDULEUSES?

- **Je réagis rapidement :** une consultation régulière de mon compte peut me permettre de détecter un incident ou une anomalie
- **Je fais opposition** à la carte bancaire piratée (0 892 705 705, service payant) ou aux chèques falsifiés (auprès de ma banque)
- **Je conteste rapidement** auprès de ma banque les opérations non autorisées ou mal exécutées, y compris des virements ou prélèvements
- **Je signale** les fraudes à la carte bancaire sur la plateforme PERCEVAL
- **Je porte plainte**, pour établir ma bonne foi.

DES SITES POUR SIGNALER

Un site pivot pour guider vos démarches…

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

www.cybermalveillance.gouv.fr

Information sur les **cyber-menaces** et les **bonnes pratiques** pour s'en protéger

Actualité de la **cyber-malveillance**

Mise en relation avec des **prestataires informatiques référencés** (prestation d'assistance payante si elle a lieu)

17 CYBER
Mon assistance en ligne

Outil de **diagnostic en ligne** de votre situation.

…et vous orienter vers le site adéquat

THÉSEE

Diagnostiquer votre situation pour **signaler** une infraction et/ou **déposer plainte**.

PERCEVAL

Signaler un usage frauduleux de votre **carte bancaire**.

https://plainte-en-ligne.masecurite.interieur.gouv.fr/

Déposer une plainte en ligne

MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER
Liberté Égalité Fraternité

PHAROS
Portail officiel de signalement des contenus illicites de l'Internet

www.internet-signalement.gouv.fr

Signaler un **contenu** ou un **comportement illicite** sur internet.

DES SITES POUR S'INFORMER

Mes questions d'entrepreneur
Le portail national de l'éducation économique, budgétaire et financière pour les entrepreneurs

www.mesquestionsdentrepreneur.fr/

Le portail de la **Banque de France** consacré à **l'Éducation Financière des entrepreneurs**

ABE info service
Assurance . Banque . Épargne

www.abe-infoservice.fr

Le site commun à la **Banque de France**, à l'**ACPR** et à l'**AMF**
Les **listes noires** et les **alertes**
Une rubrique dédiée aux **arnaques**

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Entreprendre.Service-Public.fr
Le site officiel d'information administrative pour les entreprises

www.entreprendre.service-public.gouv.fr

Le site du **service public pour les entreprises**

MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER
Liberté Égalité Fraternité

Ma Sécurité
La police et la gendarmerie nationales vous accompagnent dans vos démarches.

www.masecurite.interieur.gouv.fr

Le site et l'application de la **police et de la gendarmerie**

ARNAQUES : SÉCURISER – ALERTER – REMÉDIER ET REPRENDRE L'ACTIVITÉ.

SECURISER	Mettre en place un plan de continuité
ALERTER	Prévenir les équipes et les partenaires
REMEDIER	Trouver la source – Apporter les correctifs
REPRENDRE L'ACTIVITÉ	Surveillance accrue – Reprise progressive

Un contact de proximité

Coordonnées

Contact

Nom :
Indiquez le prénom et le nom

Numéro de téléphone :
Indiquez le téléphone

E-mail :
Indiquez l’adresse e-mail

BANQUE DE FRANCE

EUROSYSTÈME

EDUCFI

Éducation économique budgétaire et financière

BANQUE DE FRANCE

EUROSYSTÈME

EDUCFI

Éducation économique budgétaire et financière