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

Quelles sont les entreprises les plus susceptibles d'être la cible d'une cyberattaque ?

A – Les TPE/PME.

B – Les ETI.

C – Toutes les entreprises.

QUIZ

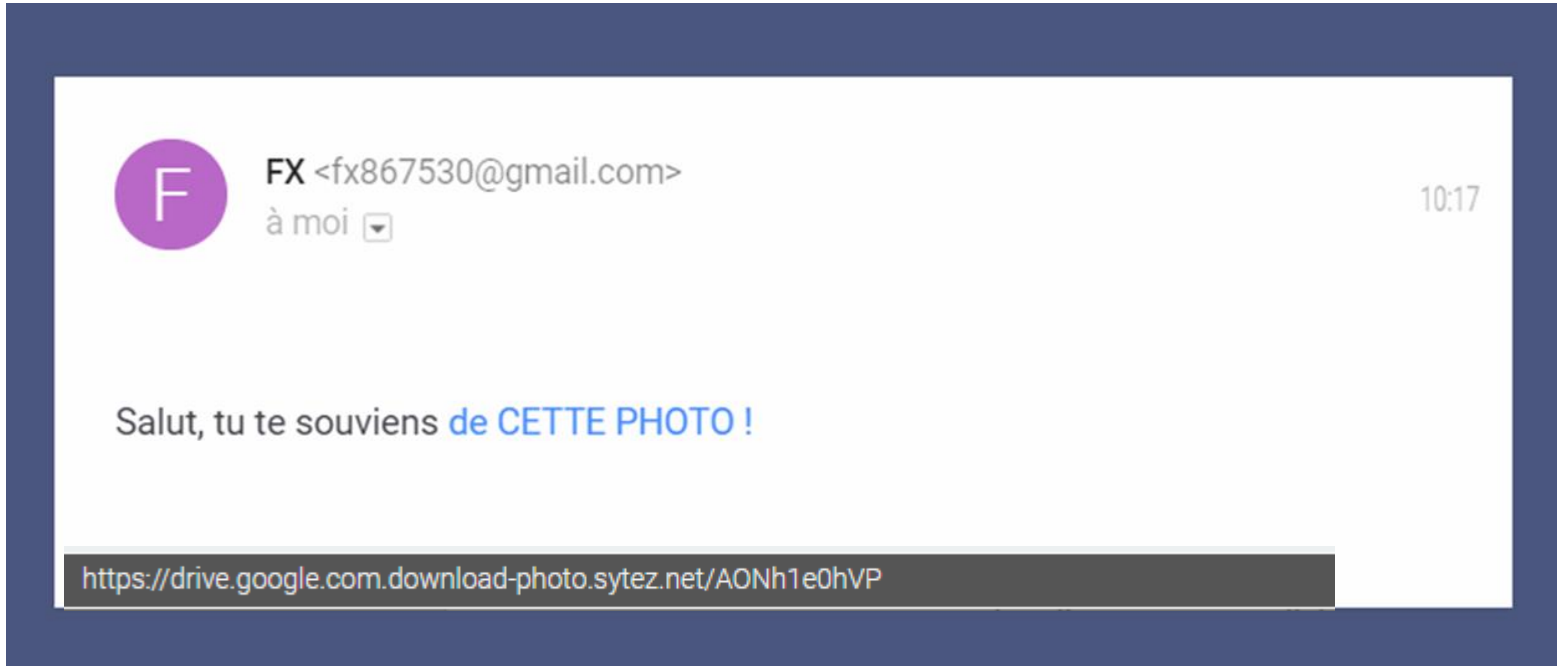
Quelles sont les entreprises les plus susceptibles d'être la cible d'une cyberattaque ?

A – Les TPE/PME.

B – Les ETI.

C – Toutes les entreprises.

QUIZ

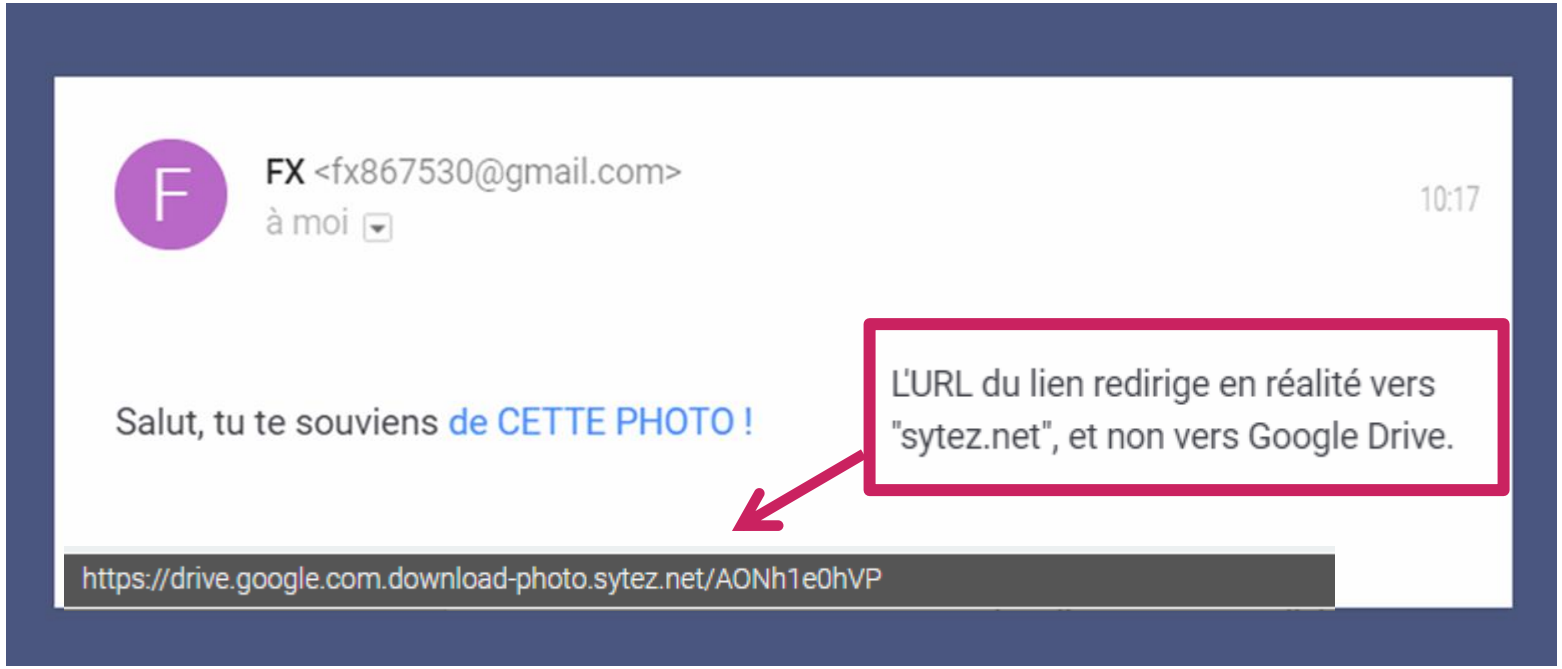


S’agit-il d’un mail frauduleux ?

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

Je travaille dans le train. Quelles précautions prendre ?

A – Se connecter au réseau public.

B – Protéger son écran d'un filtre « regards indiscrets ».

C – Rien de particulier.

QUIZ

Je travaille dans le train. Quelles précautions prendre ?

A – Se connecter au réseau public.

B – Protéger son écran d'un filtre « regards indiscrets ».

C – Rien de particulier.

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.

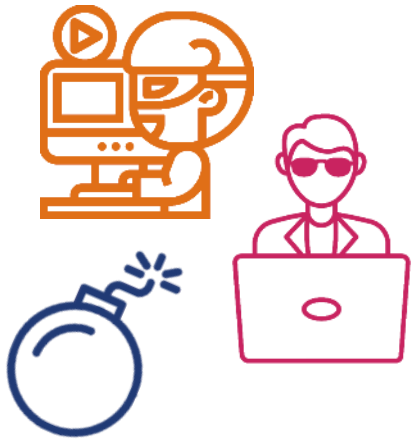
B – Une attaque sur les dossiers du répertoire.

C – Une attaque d'un réseau social.

SOMMAIRE

BANQUE DE FRANCE
EUROSYSTÈME

EDUCFI
Éducation économique budgétaire et financière

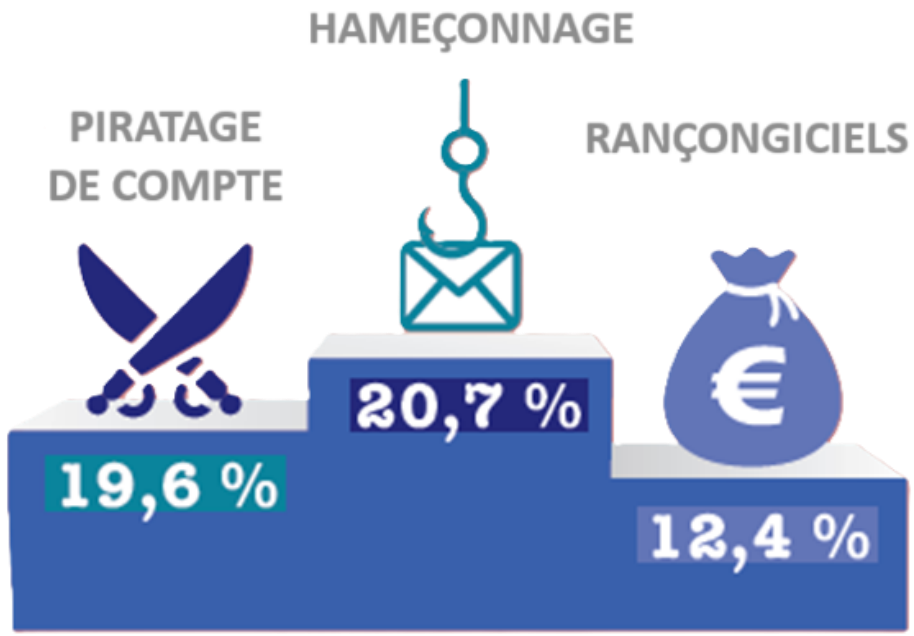


1

SAVOIR IDENTIFIER

LA CYBERCRIMINALITÉ EN QUELQUES CHIFFRES

- **53%** des entreprises françaises ont subi une attaque en 2023 *(data.gouv.fr)*
- **65%** des attaques par rançongiciel ont ciblé des entreprises en 2024 *(Cybermalveillance.gouv.fr)*.
- **Seulement 50%** des entreprises victimes portent plainte *(Baromètre, CESIN, 2024)*.



Source : cybermalveillance.gouv.fr, *Rapport d'activité 2024*

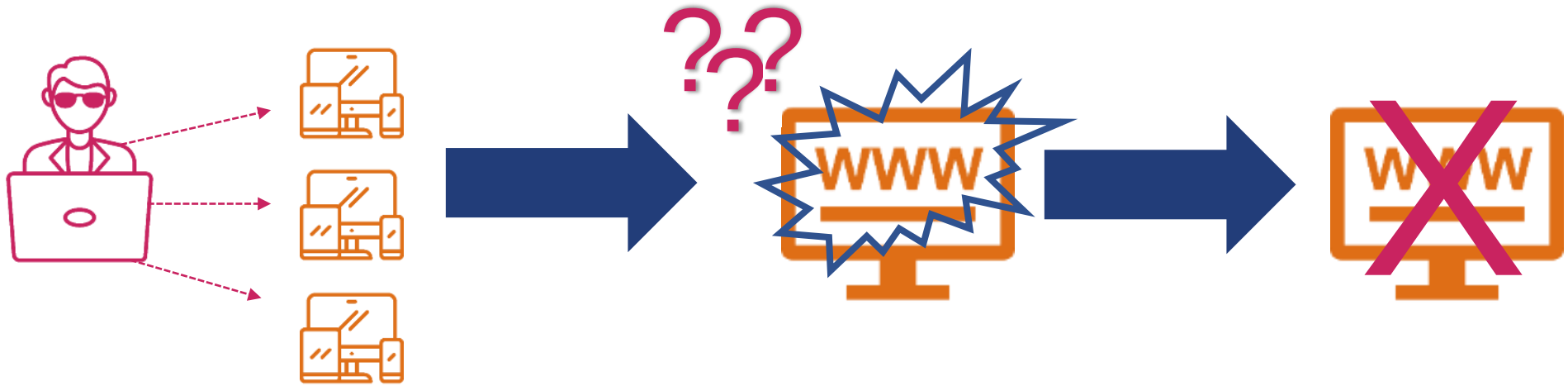
LA CYBERCRIMINALITÉ : QUELLES CONSÉQUENCES POUR L'ENTREPRISE ?

LES PRINCIPALES ATTAQUES

- **Attaque de déni de service**
- **Chantage à l'ordinateur piraté**
- **F.O.V.I. :** arnaque au faux président, au faux fournisseur…
- **Défiguration de site internet**
- **Fausse offre d'emploi**
- **Rançongiciel**
- **Piratage de systèmes informatiques**
- **Virus informatiques**
- **Usurpation d'identité**
- **Fuite de données personnelles**
- **Attaque de la chaîne d'approvisionnement**

LES ATTAQUES DDOS : « DÉNIS DE SERVICE »

- **Déroulement :** création de « BOTnet », un réseau de terminaux infectés.
- **Lancement de l'attaque :** génération d'un trafic démesuré sur le site ciblé afin de générer un nombre de requêtes trop important pour le site.
- **Conséquences :** ralentissement du système, accès interrompu aux produits ou aux services, en interne ou en externe.



LES PROGRAMMES MALVEILLANTS

- Logiciels d'espionnage « **SPYWARE** » : pénétration des systèmes d'exploitation des entreprises pour infecter une chaîne d'approvisionnement en ciblant les partenaires, les sous-traitants ou organisation de tutelle.

→ **DIVULGATION DE COORDONNEES BANCAIRES – DIVULGATION DE DONNEES SENSIBLES**

- Logiciels de contournement de l'authentification « **ROOTKIT** »

→ **VOLS DE COORDONNEES BANCAIRES – INFILTRATION D'AUTRES SYSTEMES**

- Rançongiciels « **RANSOMWARE** »

→ **BLOCAGE DE DONNEES – EXTORSION – DETOURNEMENT**

ET BIEN D'AUTRES : Déni de service, chevaux de Troie bancaire (Qbot), défacement ou défiguration de sites internet, stealer (programme de collecte des périphériques) etc… dans le but de perturber le fonctionnement de l'entreprise.

LES USURPATIONS D'IDENTITÉ (ARNAQUES AU PRÉSIDENT…)

- **Des individus :**

- Vol et utilisation de données personnelles permettant d'identifier une personne sans son accord.

Des institutions, banques, administrations :

- Tromper le destinataire du message en prenant l'identité d'une entité officielle (CAF, impôts, banques, sociétés de livraison…).

Usurpation d'identité : plus de 200 000 victimes en France par an

LES USURPATIONS D'IDENTITÉ, USURPATION DE NOM D'ENTREPRISE ET LES FAUX SITES

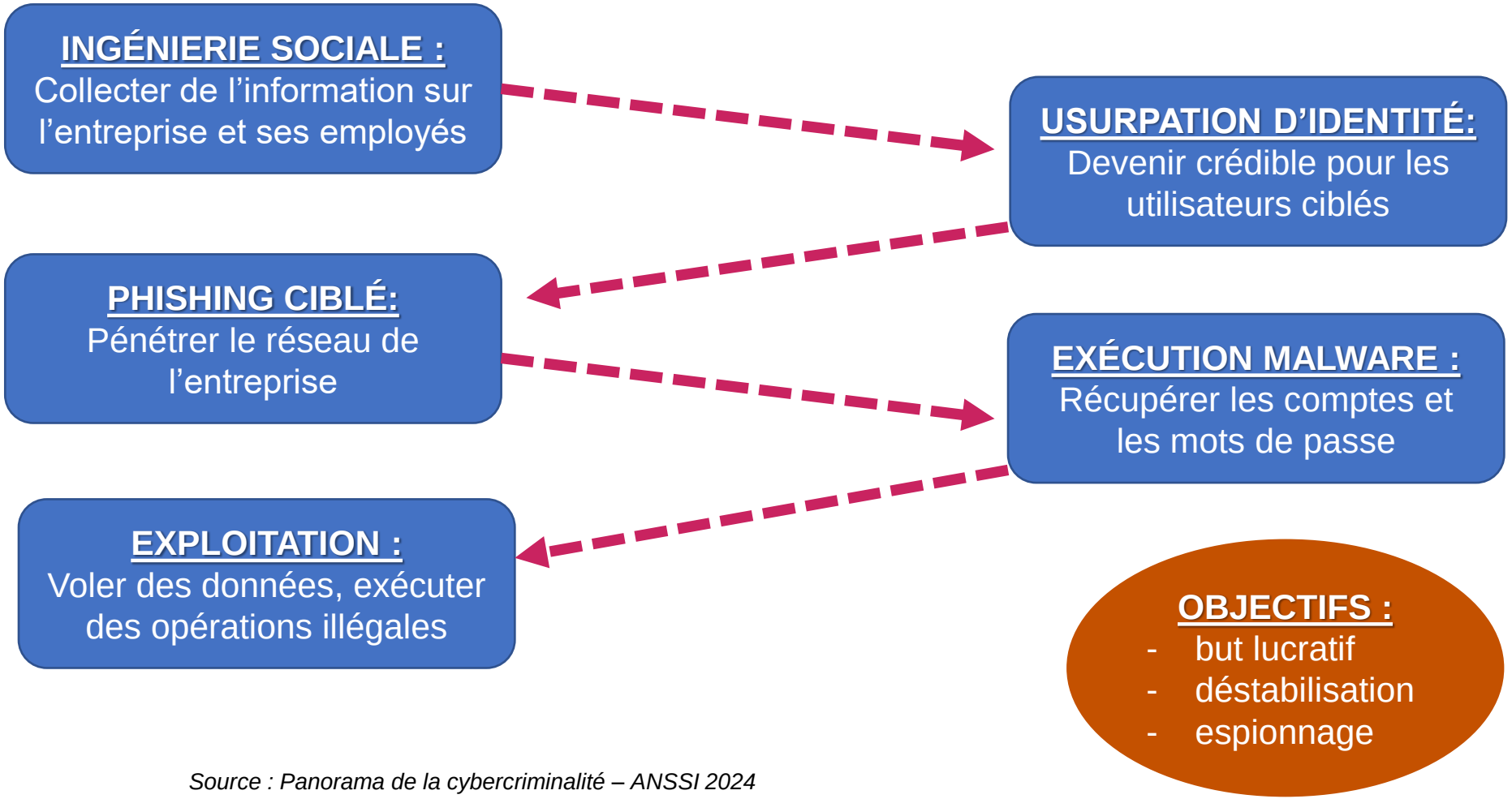
Comment s'assurer de l'authenticité d'un client / fournisseur/ partenaire d'affaire ?

10 éléments à vérifier :

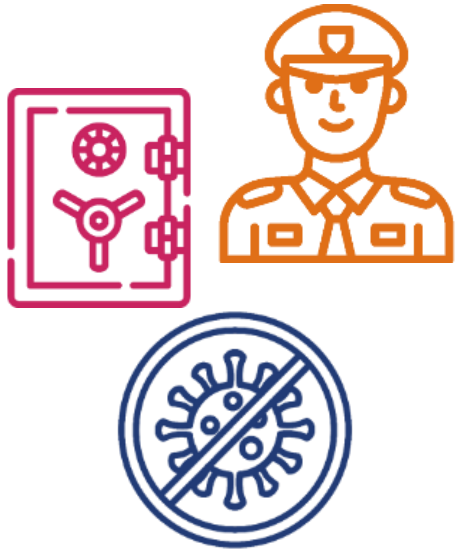
- **Interroger le registre national des sociétés**
- **Vérifier la date d'enregistrement du site web et de son propriétaire**
- **Vérifier les adresses mails et numéros de téléphone par contre-appels**
- **Consulter l'adresse physique**
- **Vérifier le mentions légales du site web**
- **S'intéresser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

LES MÉTHODES D'INGÉNIERIE SOCIALE :

- **Modus operandi des attaquants :**



Source : Panorama de la cybercriminalité – ANSSI 2024



2

SAVOIR SE PROTÉGER

BANQUE DE FRANCE
EUROSYSTÈME
EDUCFI
Éducation économique budgétaire et financière

SOMMAIRE

BANQUE DE FRANCE
EUROSYSTÈME

EDUCFI
Éducation économique budgétaire et financière

PROTÉGER SES ÉQUIPEMENTS :

- **Installer les mises à jour** (Windows, IOS, Android…) et veiller à ce qu'elles soient déployées dans l'ensemble des applications utilisées par l'entreprise.
- Installer des **logiciels de sécurité** (antivirus, anti-spywares…).
- Activer le **pare-feu**.
- **Faire des sauvegardes régulièrement** et **les tenir déconnectées du réseau** afin d'éviter qu'elles ne soient également compromises en cas de ransomware.
- **Utiliser un VPN**, dans la mesure du possible.

PROTÉGER SES ÉQUIPEMENTS

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

- Du système d’exploitation de mon ordinateur, téléphone ou tablette
- De mon antivirus
- De mon navigateur
- De mes applications

Je me méfie des **WI-FI publics** !

ÊTRE UN INTERNAUTE AVISÉ

Choisir des mots de passe difficiles à deviner

Changer les mots de passe régulièrement

Utiliser des mots de passe différents

Connaître et protéger ses données personnelles

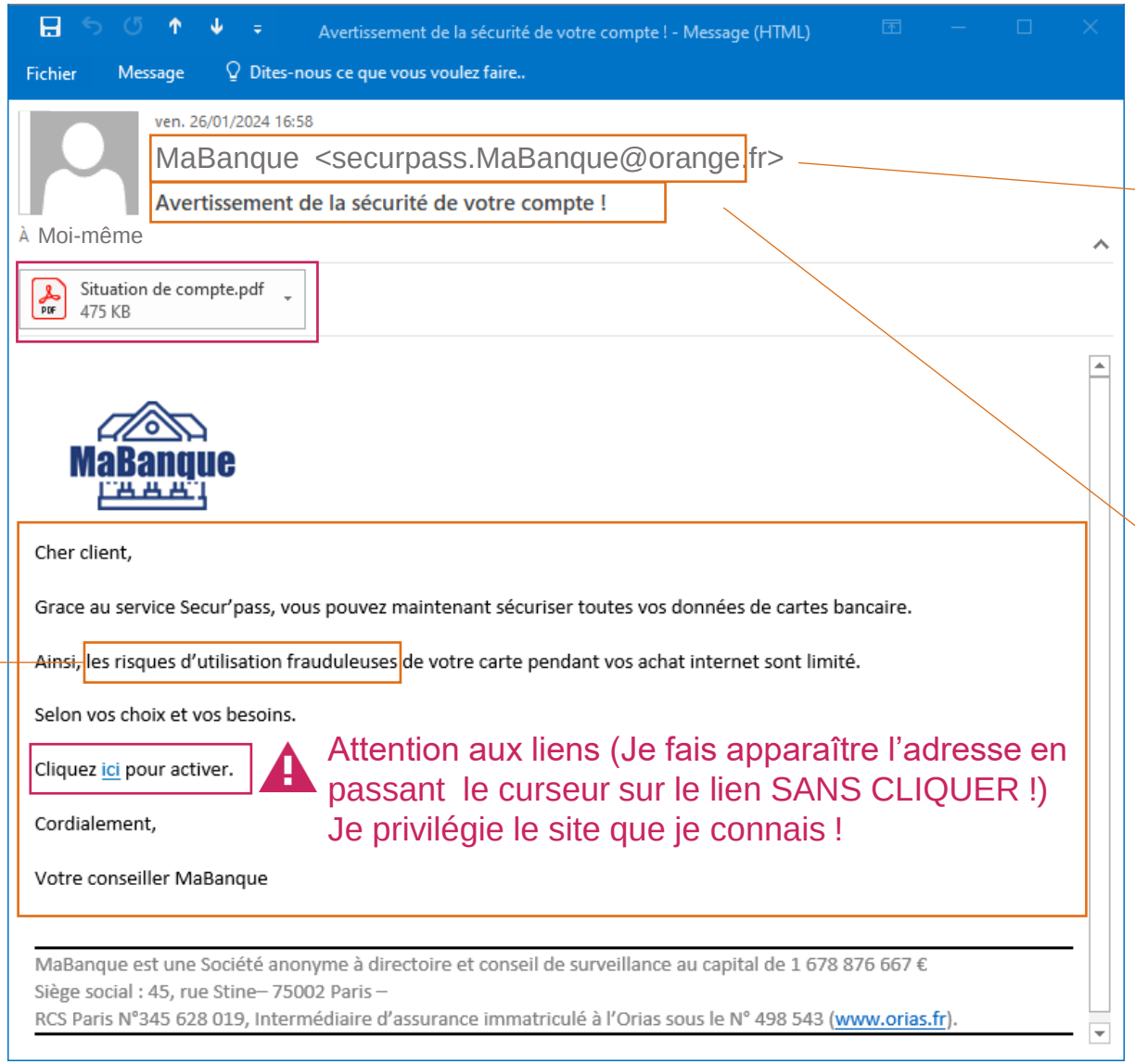
APPRENDRE À DÉJOUER LE PHISHING

- **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

Attention aux pièces jointes



Attention à l'adresse mail !

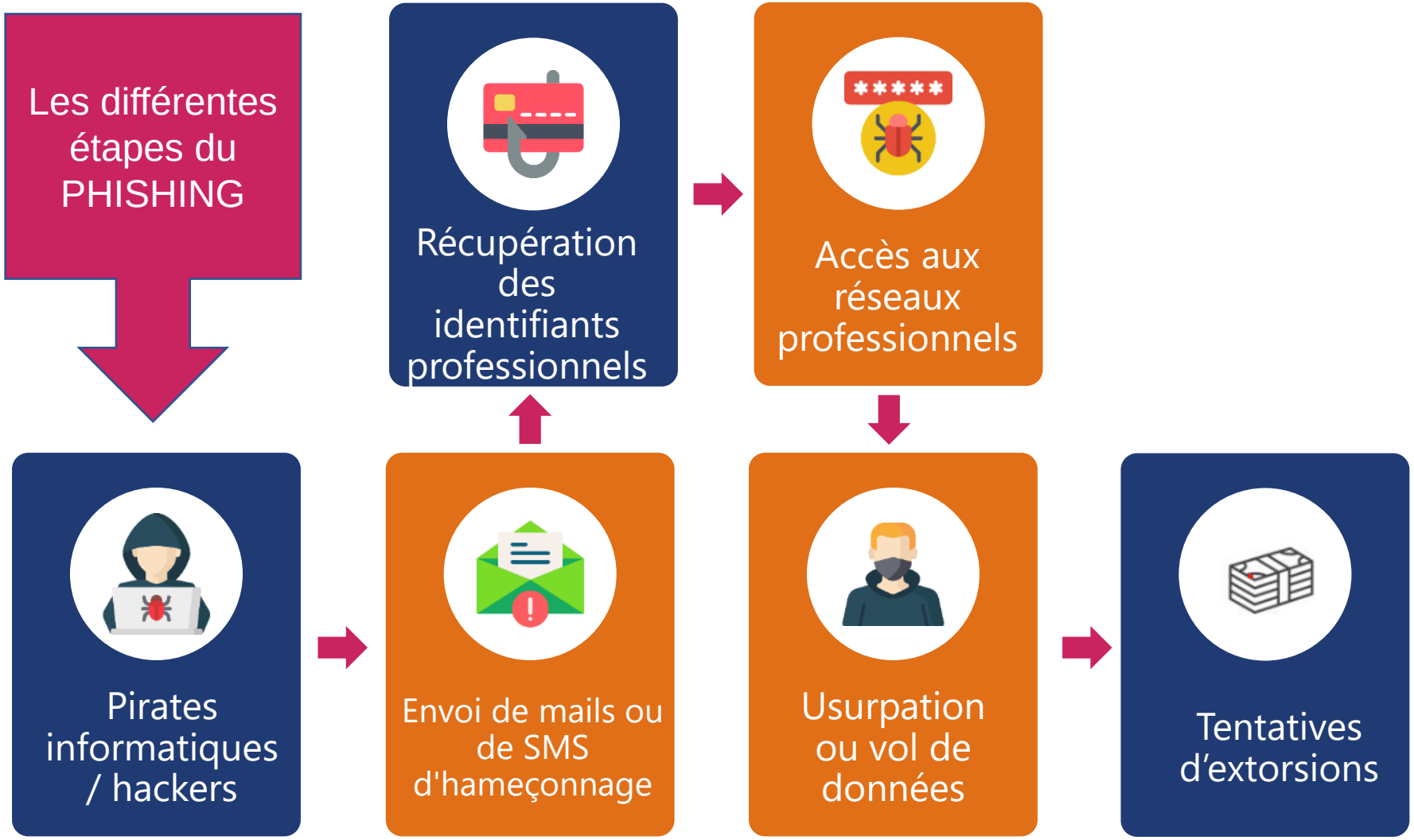
On cherche souvent à faire peur, à invoquer l'urgence, bref… à m'empêcher de réfléchir !

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

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

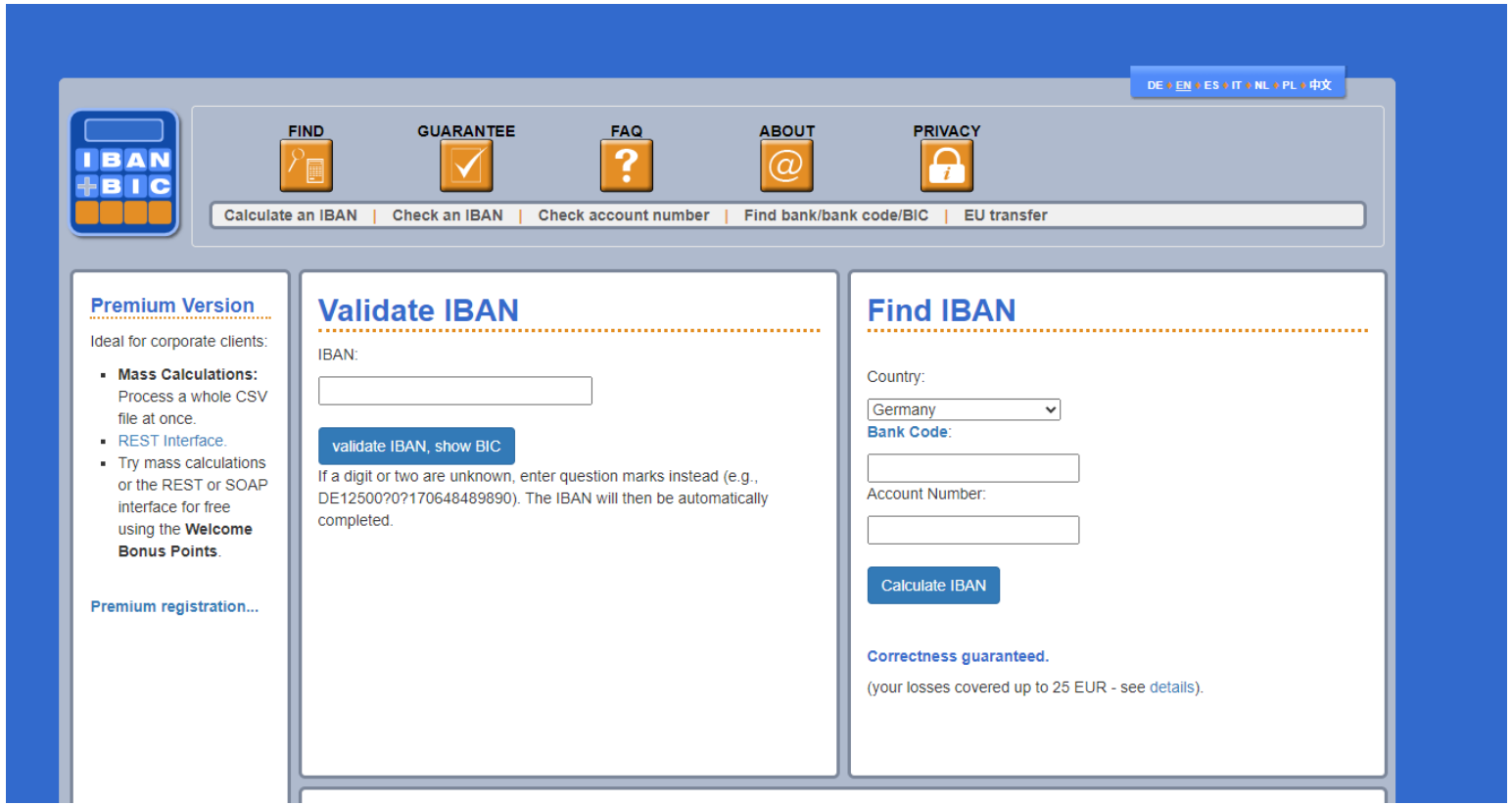
APPRENDRE À DÉJOUER LE PHISHING

Les différentes étapes du PHISHING



COMMENT DÉJOUER LES FOVI :

IBAN
Calculator



COMMENT DÉJOUER LES FOVI :

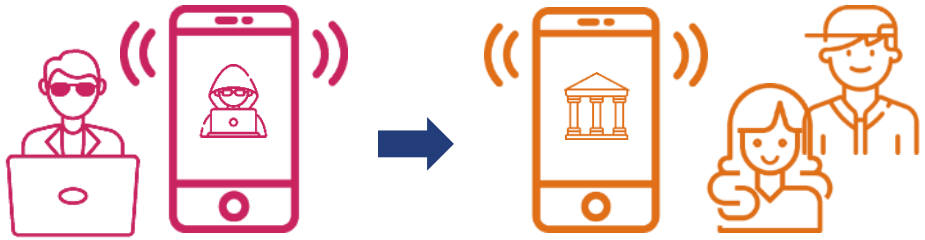
Quelques type d'IBAN…

FR76 2823 0000 : Revolut
FR76 2183 0000 : PFD Card Service Ireland Limited
FR76 1659 8000 : Nickel
…

Vous pouvez également opter pour une procédure spécifique d'intégration des IBAN avec vérification préalable.
Surtout, votre personnel doit systématiquement être formé à ce type de risque et vérifier avec un appel en cas de doute.

RECONNAÎTRE L'INGÉNIERIE SOCIALE

- Un escroc peut faire 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.
- Mais il peut également obtenir des informations à l'occasion d'**un simple appel téléphonique**.



3

SAVOIR RÉAGIR

BANQUE DE FRANCE
EUROSYSTÈME

EDUCFI
Éducation économique budgétaire et financière

PILOTER SA CYBERSÉCURITÉ EN 10 RÈGLES

Source : cybermalveillance.gouv.fr

BANQUE DE FRANCE
EUROSYSTÈME

EDUCFI
Éducation économique budgétaire et financière

COMMENT RÉAGIR FACE À UNE CYBERATTAQUE VISANT LE SYSTÈME INFORMATIQUE

La clé : réagir rapidement.

- Alerter le support informatique
- Déconnecter la machine d'internet ou du réseau informatique
- Constituer une équipe de gestion de crise
- Conserver ou faire conserver les preuves par un professionnel
- Réinstaller les systèmes touchés
- Alerter la banque
- Porter plainte
- Notifier l'incident à la CNIL
- Prévenir ses partenaires
- Ne pas payer la rançon.

COMMENT RÉAGIR FACE À UNE USURPATION D'IDENTITÉ

- Prévenir tous vos établissements financiers
- Déposer plainte (https://www.pre-plainte-en-ligne.gouv.fr)

- Contacter la Banque de France pour savoir si des incidents ont été déclarés à votre nom au FCC et FICP
- Consulter le fichier FICOBA – (auprès de la CNIL)

CNIL. PROTÉGER les données personnelles ACCOMPAGNER l'innovation PRÉSERVER les libertés individuelles

BANQUE DE FRANCE EUROSYSTÈME | EDUCFI Éducation économique budgétaire et financière

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.

BANQUE DE FRANCE
EUROSYSTÈME

EDUCFI
Éducation économique budgétaire et financière

D’AUTRES SITES POUR SIGNALER

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Signal Conso

https://signal.conso.gouv.fr/fr

Diagnostiquer et **signaler** un problème rencontré avec une entreprise.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

BLOCTEL
Espace consommateur

https://www.bloctel.gouv.fr/

Réguler le démarchage téléphonique me concernant.

33700
La plateforme de lutte contre les SMS et appels indésirables

Transfert au 33700 ou https://www.33700.fr/

Signaler les messages et les appels téléphoniques **indésirables**

signal spam

https://www.signal-spam.fr/

Signaler les courriels indésirables pour permettre aux autorités **d’identifier leur source**

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**

ASSURANCE BANQUE EPARGNE Info SERVICE

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.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**

BANQUE DE FRANCE EUROSYSTÈME | EDUCFI Éducation économique budgétaire et financière

QUELQUES NUMÉROS DE TÉLÉPHONE

- **3414** — Accès aux services aux entreprises de la Banque de France
  Difficultés et incidents bancaires, informations sur les questions de banques et d'assurances
- **08 09 540 550** — DGCCRF (numéro d'appel non surtaxé)
  La ligne de la DGCCRF
- **0 805 805 817** — Info Escroqueries (appel gratuit)
  La ligne du site de la police et de la gendarmerie
- **116 006** — Aide aux victimes (appel gratuit)
  Permet aux victimes d'infractions, d'accidents ou catastrophes de bénéficier d'informations et d'une écoute par des professionnels.

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