esea
LA E-SANTÉ NOUVELLE-AQUITAINE

URPS
MÉDECINS LIBÉRAUX
Nouvelle-Aquitaine

Ingénierie sociale : quand la cyberattaque passe par l'humain

Web'1H

Alexina MELI & Gabrielle DATTEE

Direction Cybersécurité – GRADeS ESEA N-A

Docteur Philippe DURANDET

Président de la Commission I-Santé

Emmanuel BATAILLE

Directeur de l'URPS Médecins Libéraux Nouvelle-Aquitaine

14 octobre 2025

Pourquoi vous cibler ?
Que valent nos données ?

Carte de crédit
20 $ à 60 $

Comptes de paiements en ligne
1 $ à 100 $

Boites mails et comptes de réseaux sociaux
1$ à 65 $

Dossiers médicaux ou informations médicales
1 $ à 380 $

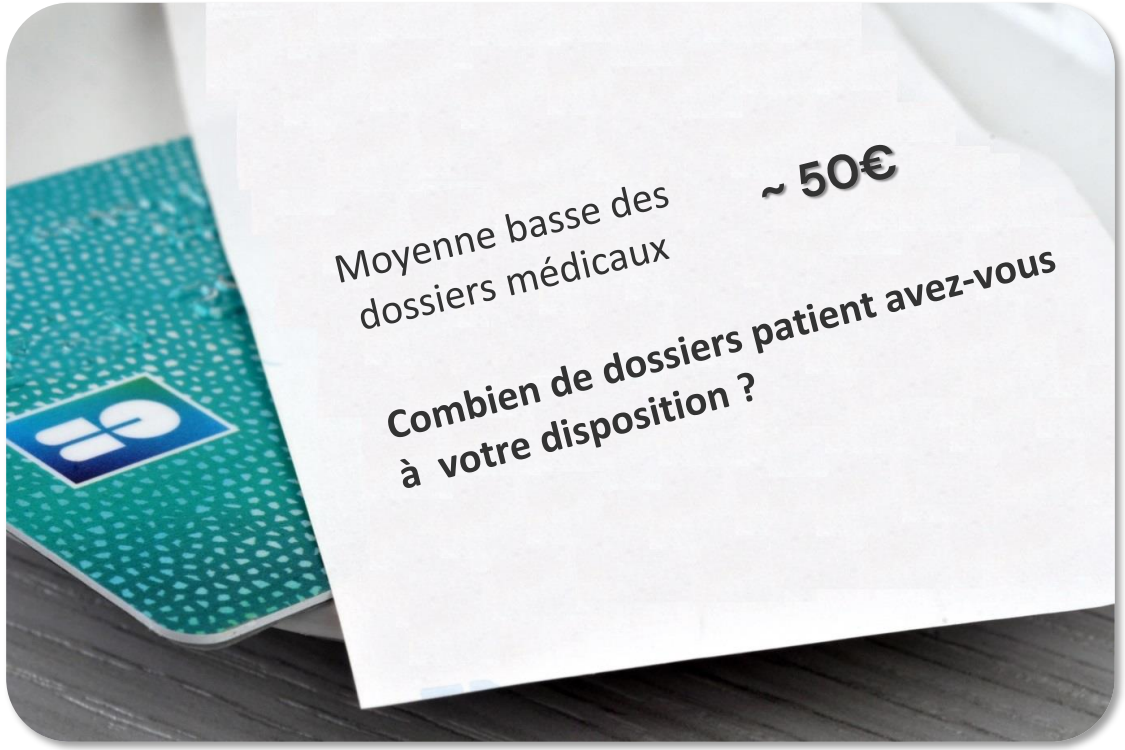
Accès aux comptes bancaires
0,5% à 10 % de sa valeur

Comptes de jeux vidéo
1 $ à 12 $

Scan ou document physique de papiers d'identité,
1 $ à 3,000$

Comptes de streaming
1$ à 20 $

Cartes cadeaux
10 % à 50 % de sa valeur



Qu’est-ce que l’ingénierie sociale ?

- Dans le contexte de la cybersécurité, l’ingénierie sociale est une **technique de manipulation psychologique utilisée pour tromper une personne** afin de l’amener à divulguer des informations sensibles ou à réaliser une action qui compromet la sécurité de son système d’information.

Pourquoi c’est efficace ?

L’erreur humaine est impliquée dans plus de **90%** des incidents de sécurité !
L’être humain est le maillon faible : même les systèmes les plus sécurisés peuvent être contournés si une personne est trompée.

Facilité d’exécution : les attaquants n’ont pas besoin de compétences techniques avancées.

Rentabilité : une campagne de phishing bien conçue peut toucher des milliers de personnes à moindre coût.

Difficulté de détection : les attaques semblent provenir de sources de confiance (banques, collègues, institutions officielles).

Pourquoi cela fonctionne si bien ?

Les attaquants exploitent des **leviers psychologiques universels**. Par exemple, ils jouent sur :

- **L'urgence** : nécessité d'agir immédiatement sous peine de conséquences.

« Mise à jour obligatoire sous 48h sous peine de perdre vos données patients »

- **La curiosité** : promesse d'une information exclusive ou d'un fichier intriguant.

« Cas clinique rare – à voir absolument ».

- **La peur** : menace de fermeture de compte, d'amende, d'incident grave.

« Une fraude a été détectée dans vos télétransmissions »

- **La confiance** : usurpation de l'identité d'un collègue, d'un supérieur ou d'une institution.

« Besoin de l'avis d'un confrère en urgence »

- **La récompense** : promesses de gains financiers, cadeaux, primes.

« Une réduction sur le matériel médical »

Les principales menaces

Phishing

e-mail frauduleux qui imite des organismes connus

But : inciter à cliquer sur un lien malveillant ou une pièce jointe frauduleuse pour voler des données

Phishing de masse VS Phishing ciblé (spear phishing)

Vishing

(**phishing vocal**) = appels téléphoniques frauduleux.

Fraude au faux conseiller bancaire, au faux support technique

Smishing

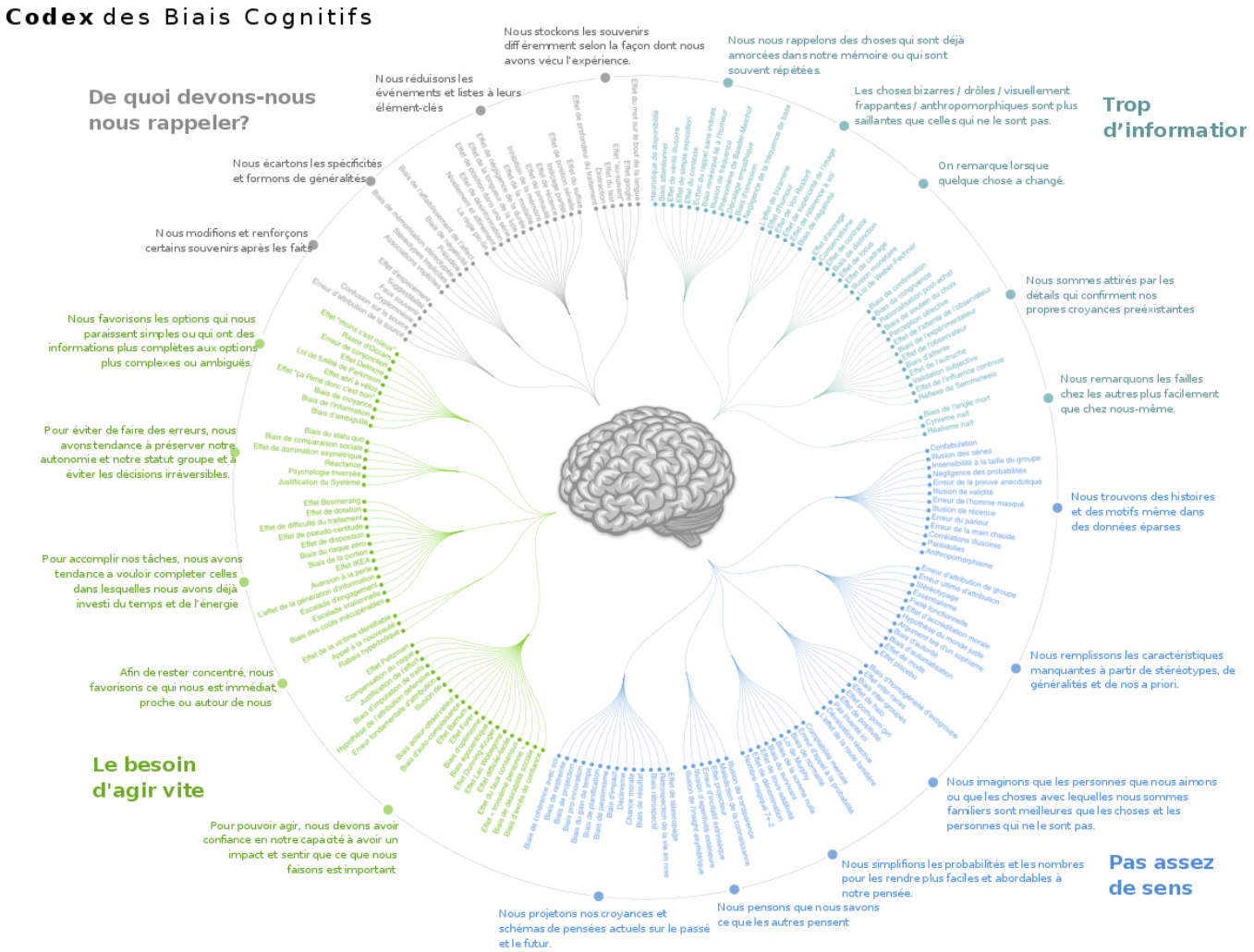
Même principe que le phishing mais via SMS.

« Votre colis ne rentre pas dans la boîte aux lettres… »

Et aussi dans le monde physique !

Dépôt d'une clé USB infectée dans un endroit stratégique (parking)

Comment cela fonctionne ?
Nous avons tous des biais cognitifs



esea
LA E-SANTÉ NOUVELLE-AQUITAINE

URPS MÉDECINS LIBÉRAUX Nouvelle-Aquitaine

7 moyens pour déstabiliser sans peine

1) Autorité

Principe : nous **obéissons** instinctivement aux injonctions si elles émanent de figures d'autorité (CPAM, éditeur, banque).

- Exemple : « mise à jour urgente et importante de votre logiciel métier – blocage de votre carte vitale si vous ne répondez pas »

- **Antidote** : contactez l'interlocuteur par un autre moyen. Rappel via annuaire/numéro du contrat (jamais le n° reçu).

2) Urgence

Principe : la **pression temporelle** réduit l'esprit critique.

- Exemple : « Blocage Ameli Pro dans 24 heures »

- **Antidote** : Prendre le temps de réflexion (pause, source, preuve, canal officiel, différer).

Pas de décision sous pression ++

Action + pression temporelle → fraude probable.

3) Sympathie entre pairs

Principe : on dit oui à quelqu'un de **sympathique / proche**. Confiance accrue envers nos pairs. Volonté d'aider.

- Exemple : Demande d'un dossier patient de la part d'un « confrère » dont l'identité a été usurpée.

- **Antidote** : mêmes règles pour tous ; aucune exception « pour dépanner ». Recontacter par un autre canal.

4) Fatigue décisionnelle

Principe : **Surcharge et fin de journée** = décisions rapides et risquées.

- Exemple : Ignorer l'alerte de sécurité à 20h.
- **Antidote** : Vigilance sur les informations reçues en fin de journée/semaine.

5) Engagement (pied-dans-la-porte)

Principe : un **petit « oui »** en entraîne un plus grand.

- Exemple : « Confirmez juste votre identité… puis partagez le code à usage unique (OTP) »

- **Antidote** : ne jamais partager de code de double authentification ni de mot de passe avec un tiers

6) Jargon « technique »

Principe : discours très « **professionnel/technique » qui semble légitime**.

- Exemple : « Certificat Ségur non conforme : lancez Anydesk pour configurer votre tunnel TLS »

- **Antidote** : Toujours exiger des explications claires. Aucune prise en main à distance hors ticket planifié par l'éditeur.

7) Curiosité & gratification

Principe : attrait pour pièce jointe /lots/fichiers intrigants.

- Exemple : « Compte-rendu patient / résultats labo en PJ (.ZIP) »
- **Antidote** : n'ouvrir que via les canaux attendus (MSSanté / plateformes labo ou radio).


Bonjour,
Un dossier patient vous a été transmis par un confrère, pour avis ou suivi médical.
Pour en prendre connaissance, veuillez télécharger le fichier joint sur notre portail sécurisé .

Cordialement,

CENTRE HOSPITALIER
SECRÉTARIAT

Les bons réflexes

Règles d’or

- Les mots de passe et codes **Pro Santé Connect / eCPS / Ameli Pro / Banque** ne se partagent **jamais**.
- Je ne **clique pas**, je **n’ouvre pas la pièce jointe**, je **n’installe pas de logiciel**.
- **Je rappelle** via un **numéro officiel** (annuaire/contrat) — **jamais** celui reçu.
- Je vérifie **l’identité de mon interlocuteur**.

esea
LA E-SANTÉ NOUVELLE-AQUITAINE

URPS
MÉDECINS LIBÉRAUX
Nouvelle-Aquitaine

Merci de votre attention !

Contactez-nous : cybersecurite@esea-na.fr

Protégez vos patients, vos données et votre cabinet : adoptez ces réflexes simples.

1. Vérifiez l'identité
- Ne partagez jamais d'informations sensibles sans confirmer l'identité du demandeur.
- Utilisez les canaux officiels pour valider les demandes.

2. Méfiez-vous des urgences suspectes
- Les cybercriminels exploitent la pression du temps.
- Prenez toujours le temps de vérifier avant d'agir.

3. Protégez vos mots de passe
- Ne réutilisez jamais vos mots de passe professionnels.
- Activez l'authentification à deux facteurs (2FA).

4. Soyez vigilant face aux emails et liens
- Ne cliquez pas sur les liens ou pièces jointes non sollicités.
- Vérifiez l'adresse de l'expéditeur et les anomalies dans le message.

5. Sécurisez vos appareils
- Verrouillez vos ordinateurs, tablettes et smartphones.
- Maintenez vos logiciels à jour.

6. Limitez le partage d'informations
- Ne divulguez que le strict nécessaire.
- Évitez les discussions sensibles dans les espaces publics.

7. Questionnez les demandes inhabituelles
- Même si la demande semble venir d'un collègue ou d'un supérieur.
- Contactez directement la personne par un canal connu.

8. Signalez tout incident
- Toute suspicion d'ingénierie sociale doit être remontée immédiatement.
- Suivez les procédures internes de votre établissement.

9. Formez-vous régulièrement
- Participez aux sessions de sensibilisation et aux simulations de phishing.
- Restez informé des nouvelles techniques utilisées par les cybercriminels.

10. Adoptez la culture de la prudence
- La sécurité est l'affaire de tous.
- Encouragez vos collègues à adopter les mêmes réflexes.

esea
LA E-SANTÉ NOUVELLE-AQUITAINE

URPS
MÉDECINS LIBÉRAUX
Nouvelle-Aquitaine

Se protéger du phishing

Quelques bonnes pratiques pour détecter un mail de phishing :

- Méfiez-vous des mails ou demandes inattendus
- Ne vous laissez pas piéger par la menace ni l'urgence
- Vérifiez l'adresse mail de l'expéditeur
- Au moindre doute, contactez l'expéditeur par un autre moyen (téléphone)
- Passez le curseur de la souris sur l'URL du lien, sans cliquer dessus
- Ne partagez pas d'informations personnelles / sensibles

PENSER
avant de
CLIQUER

Ressources utiles

Ressources	Descriptif	Liens
Plateforme e-learning ELEA+	Modules de formation du GRADeS ESEA dédiés à la cybersécurité	https://elea.esea-na.fr/local/explore/?field%5B0%5D=competence&value%5B0%5D=3&sort=popularity
Cybermalveillance	Assistance et prévention du risque numérique	https://www.cybermalveillance.gouv.fr/
CNIL	Notification de violation de données sensibles. Aide à la conformité RGPD	https://cnil.fr/fr
Annuaire Santé / RPPS	Recensement des professionnels de santé enregistrés dans le RPPS	https://annuaire.sante.fr/web/site-pro
Mémento de la sécurité pour les professionnels de santé libéraux	Guide de bonnes pratiques rédigé par l'ANS	https://esante.gouv.fr/actualites/lans-publie-un-memento-de-securite-informatique-pour-les-professionnels-de-sante-en-exercice-liberal