

JOURNÉE EXERCICE MÉDICAL LIBÉRAL

L'exercice libéral de demain se construit aujourd'hui

Cybersécurité:
*un réflexe essentiel pour
exercer en toute tranquillité*

Les intervenants



Dr. Philippe Durandet

Cardiologue

Elu URPS ML NA

Président de la commission i-santé



M. Nicolas Chaleyssin

Assistant projet cybersécurité

ESEA



Mme Blandine Roquebert

Assistante de projets

URPS chirurgiens-dentistes NA

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).



Qu'est-ce que les biais cognitifs ?

Un biais cognitif est un processus de pensée automatique et souvent inconscient qui façonne notre jugement et notre perception. Ces mécanismes mentaux nous aident à prendre des décisions rapidement, mais peuvent aussi nous induire en erreur.

Ils influencent nos choix, en particulier dans des situations où nous sommes confrontés à une surcharge d'informations ou à des décisions rapides.



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 intrigant.
« 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 »

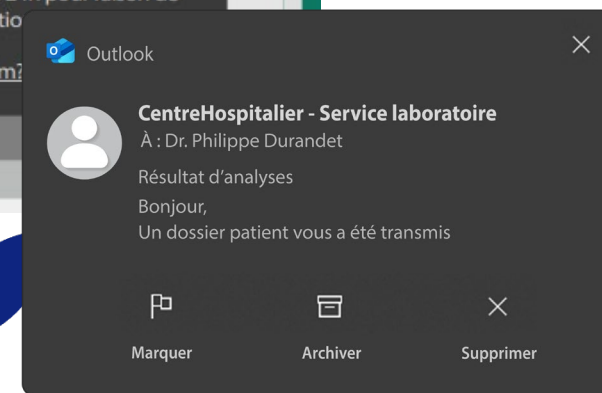


Les principales menaces

Le Smishing



Le Phishing



🔊 Ignorer

🔒 Bloquer

🗑 Supprimer

📁 Archiver

🚨 Signaler

↩ Répondre

↩ Répondre à tous

➡ Transférer

📅 Planifier avec Copilot

🗓 Réunion

💬 Conversation instantanée

👥 Partager dans Teams

🔍 Zoom

📁 Déplacer

🗑 Ranger

📁 Règles

⚡ Actions rapides

✉ Lu / non lu

🏷 Catégoriser

🚩 Drapeau

⚙ Stratégie

🕒 Répéter

🖨 Imprimer

>

^

Copilot

Résultat d'analyses

Résumé par Copilot

×

C

Centre Hospitalier - Service laboratoire

À : 🟢 BAUER-DUPUY Laura

😊

↩ Répondre

↩ Répondre à tous

➡ Transférer

🔗

📄

⋮

Ven 05/09/2025 12:30

📘

Vous avez transféré ce message le Ven 21/11/2025 12:11

Afficher une conversation

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,



↩ Répondre

➡ Transférer

Les 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.



Se protéger du 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
(ex: téléphone)

Passez le curseur de la
souris sur l'URL du
lien, sans cliquer
dessus



Ressources utiles

Guide de conformité des contrats informatiques

← Ressources URPS ML NA →

Autodiagnostic « ma pratique cyber »

Ressources ESEA ou nationales	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



JOURNÉE EXERCICE MÉDICAL LIBÉRAL

L'exercice libéral de demain se construit aujourd'hui

MERCI !

Pourquoi vous cibler ? Que valent nos données ?



Carte de crédit
20 \$ à 60 \$



Comptes de
paiements en
ligne
1 \$ à 100 \$



Boîtes 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

