Cybersécurité & Changement de Comportement

Pourquoi TOI fais-tu la différence ?

La cybersécurité ne concerne pas la technologie. Elle concerne les personnes.

Steven Debruyn
Domain Lead - Cybersecurity Awareness
CISO Office SNCB

Inspirational Session

En route.
Vers mieux.

95%

of Breaches are Caused by Human Error

Source: Cybint

Les hackers ciblent les personnes, pas les pare-feux.

Vous êtes notre première ligne de défense

La cybersécurité est la responsabilité de tous

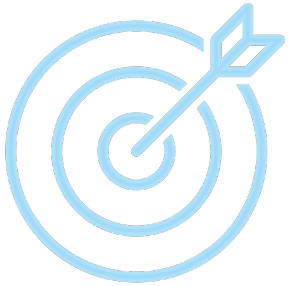
Vous êtes notre première ligne de défense

HUMAN FIREWALL

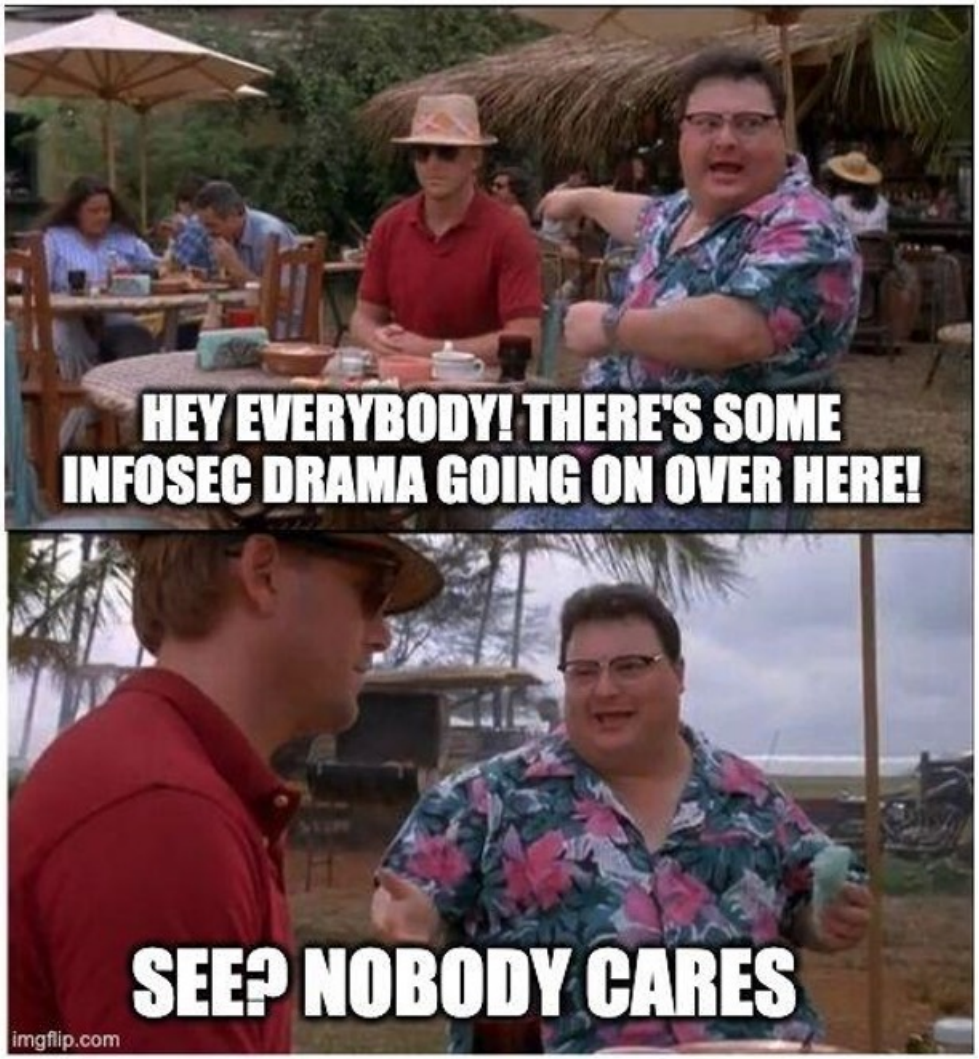

Website URL
Download AntiVirus
Secure data folder
Checking Trusted Wi-Fi connection
CYBER SAFETY
MISTAKES IN DELIVERING
CYBER SECURITY
AWARENESS CAMPAIGNS
Corporate
• Corporate communication & Public Affairs
• Ypto • Digitalisering • IT
Un compte bien verrouillé est plus difficile à hacker !
De nos jours, il est courant de devoir créer un compte avec un identifiant et un mot de pass...
LEES MEER
VORIGE
VOLGENDE
HOW TO BUILD A
CYBER SECURITY
AWARENESS
PROGRAM
CYBERSECURITY
AWARENESS MONTH
NAVIGATING
CYBER THREATS

Souvenez-vous de cette scène

C’est une bonne référence pour montrer que le personnel ne s’en soucie pas si cela n’a aucun impact direct sur eux.



- Pas de temps
- Pas d’intérêt
- Je m’en fiche
- Aucun avantage pour moi
- Je préfère que les choses restent comme avant

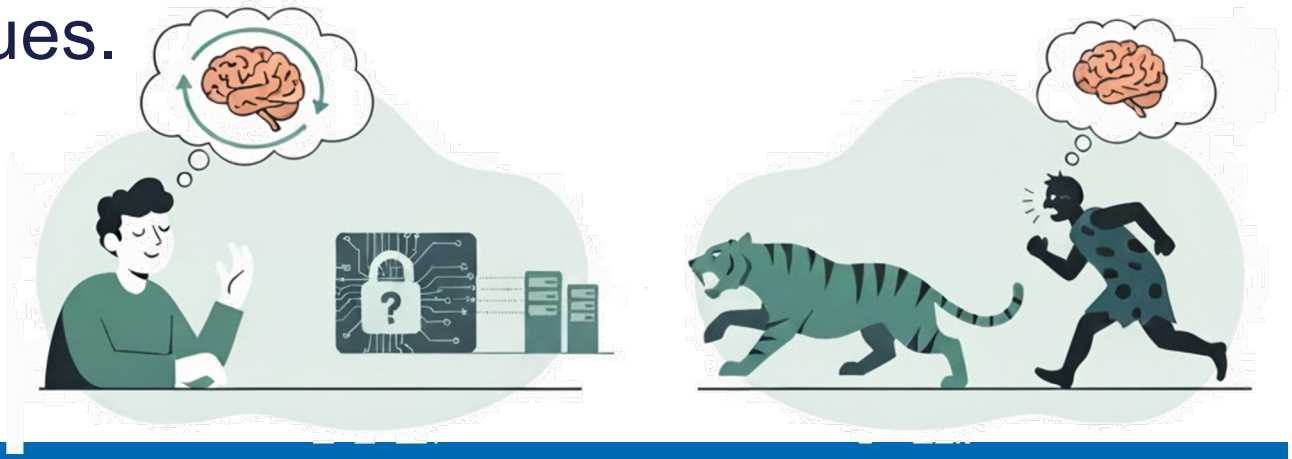


Mais attends… nous allons découvrir comment changer cela.


MINDSET
CHANGING...

Pourquoi il est si difficile de changer de comportement

- Les gens sont des créatures d'habitude.
- La cybersécurité semble abstraite, lointaine, technique, « pas mon travail ».
- L'évolution du cerveau : nous réagissons au danger immédiat, pas aux risques numériques.



La psychologie du comportement

Comportement = motivation + capacité + déclencheur
(Modèle de comportement de Fogg)

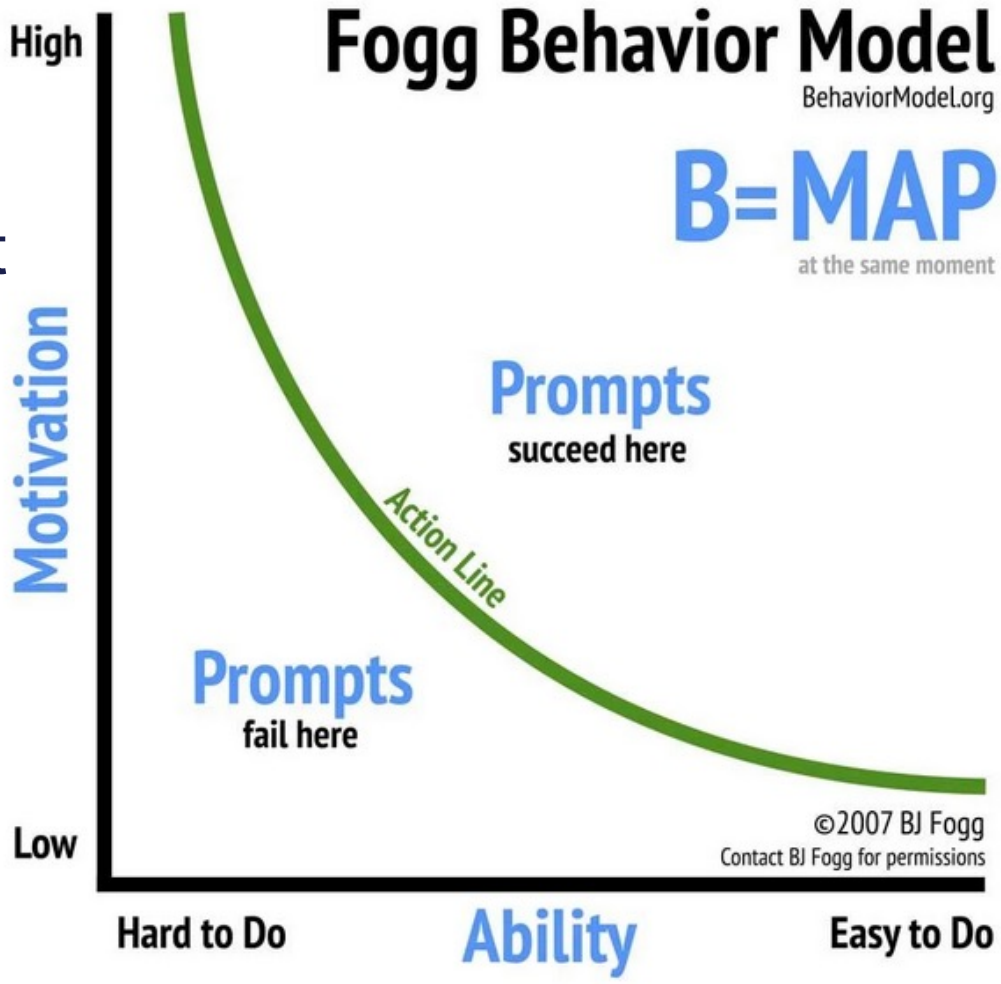
Si quelque chose semble difficile, flou ou sans intérêt
→ aucune action.

Les gens ne changent que lorsqu'ils en tirent
un bénéfice pour eux-mêmes.

Le comportement se produit lorsque la motivation, la capacité et un déclencheur se rencontrent en même temps.

Lorsqu'un comportement ne se produit pas, au moins un de ces trois éléments fait défaut.

Dr. BJ Fogg, PhD, Stanford University,



Ce qui ne fonctionne pas avec la sensibilisation classique

- Modules e-learning longs (ennuyeux).
- Menacer avec des politiques (résistance).
- Trop technique, trop éloigné du quotidien.
- Focus sur le « devoir », pas sur le « vouloir ».

The Missing Link

WHAT'S IN IT FOR ME ?

- Les gens ne changent que lorsqu'ils perçoivent un bénéfice pour eux-mêmes.
- La vie privée est un puissant moteur.
- Si vous apprenez des pratiques sécurisées pour vous-même
  → vous les appliquez aussi au travail.

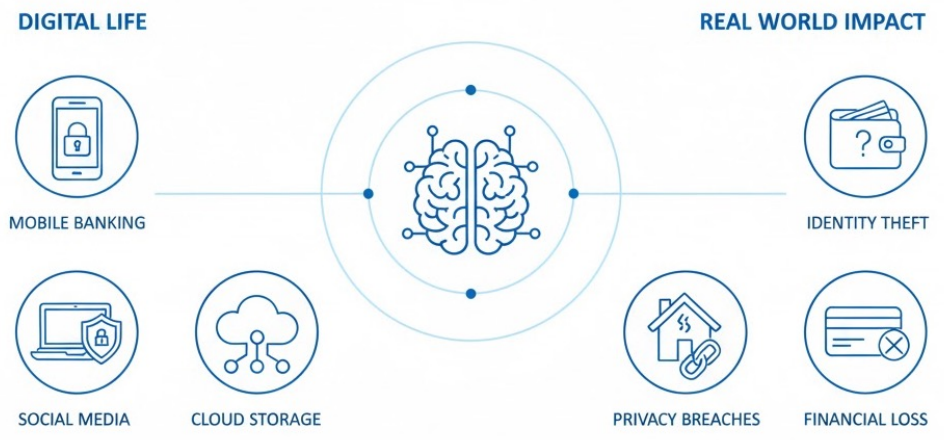
Technique 1 : Rendez-le personnel

Utilisez des exemples tirés de la vie privée :

« Comment réduire le risque que votre compte bancaire soit vidé ? »
« Comment protéger les photos de vos enfants ? »
« Comment éviter que quelqu'un prenne le contrôle de votre WhatsApp ? »

Si quelqu'un sécurise mieux son smartphone

→ automatiquement il adopte un meilleur comportement au travail.

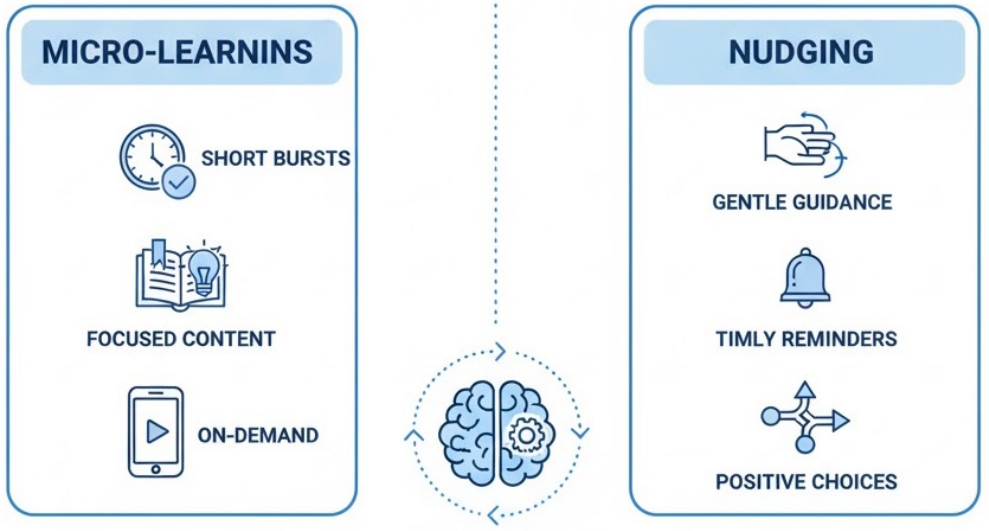


Technique 2 : Micro-learnings et nudging

Petites informations faciles à digérer.

Nudges : petits coups de pouce subtils
(par ex. avertissement si le mot de passe est faible).

Exemple :
Gmail affiche
« Cela ressemble à du phishing ».



Technique 3 : Gamification

Systèmes de points, badges, scores.

Compétitions entre équipes : qui détecte le plus de mails de phishing ?

Les gens aiment la compétition, même modérée.

TURN TASKS INTO TRIUMPHS.

Technique 4 : Preuve sociale

Les gens calquent leur comportement sur celui des autres.

« 80 % de vos collègues ont activé la MFA » → augmente l'adoption.

Modèles : des managers qui participent activement.

THE POWER OF INFLUENCE

Technique 5 : Abaissez la barrière

Facilitez le comportement sécurisé :

- Gestionnaires de mots de passe.
- MFA avec biométrie.
- La sécurité comme paramètre par défaut dans les outils.
- « Le comportement change plus vite lorsque la technologie aide. »

Technique 6 : Vous pouvez y gagner quelque chose

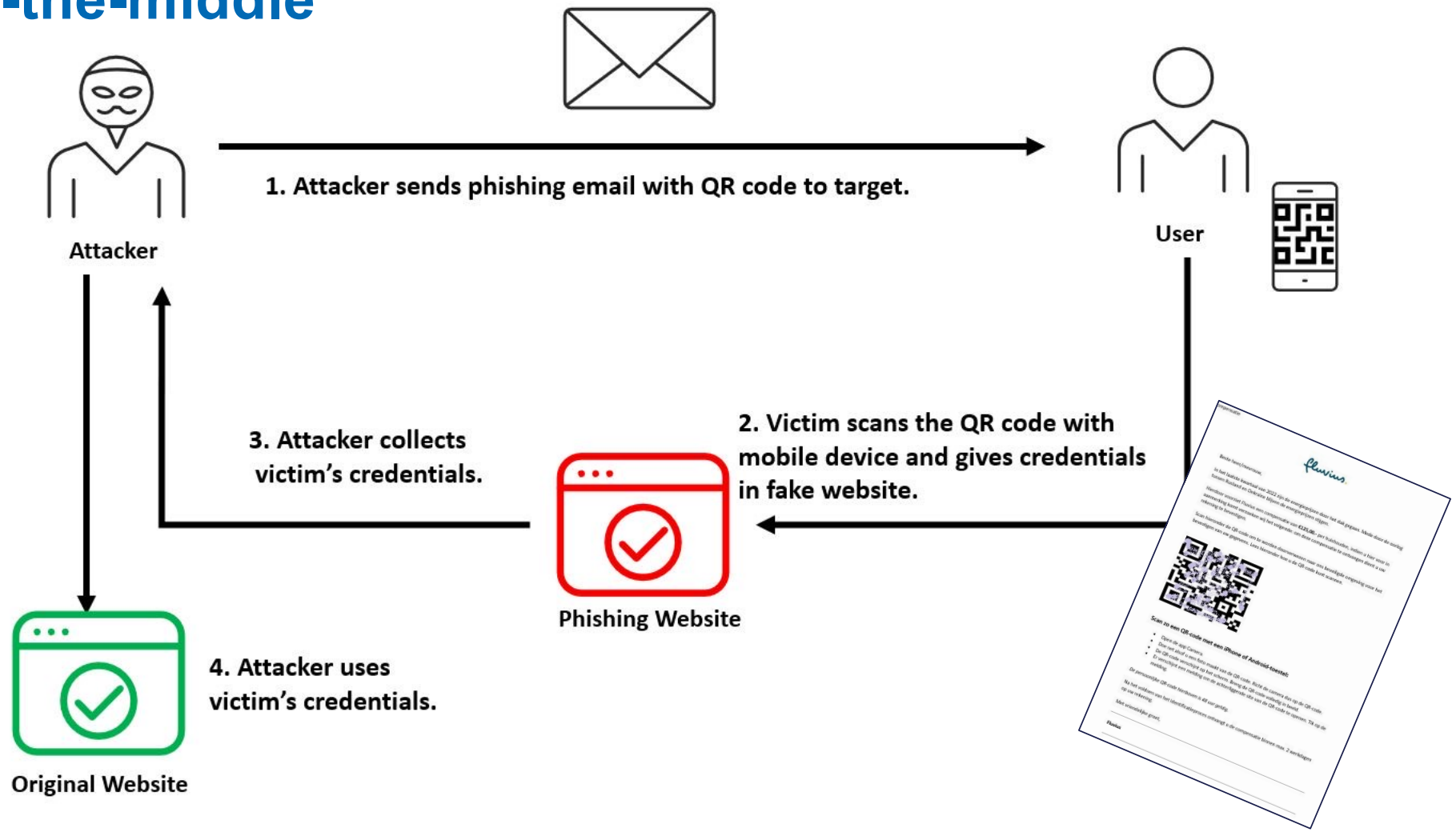
Il ne doit pas s'agir d'un gros budget.

J'ai fait le test avec notre Quiz CISO
Plus de 3 000 participants parce qu'il y avait cinq duotickets de cinéma à gagner.

(Budget = 120 euro)

Expliquez exactement comment fonctionne le phishing et ce qu’il y a derrière, afin qu’ils comprennent.

Man-in-the-middle



C’est l’heure d’une démonstration de hacking en direct !

Deux règles importantes !

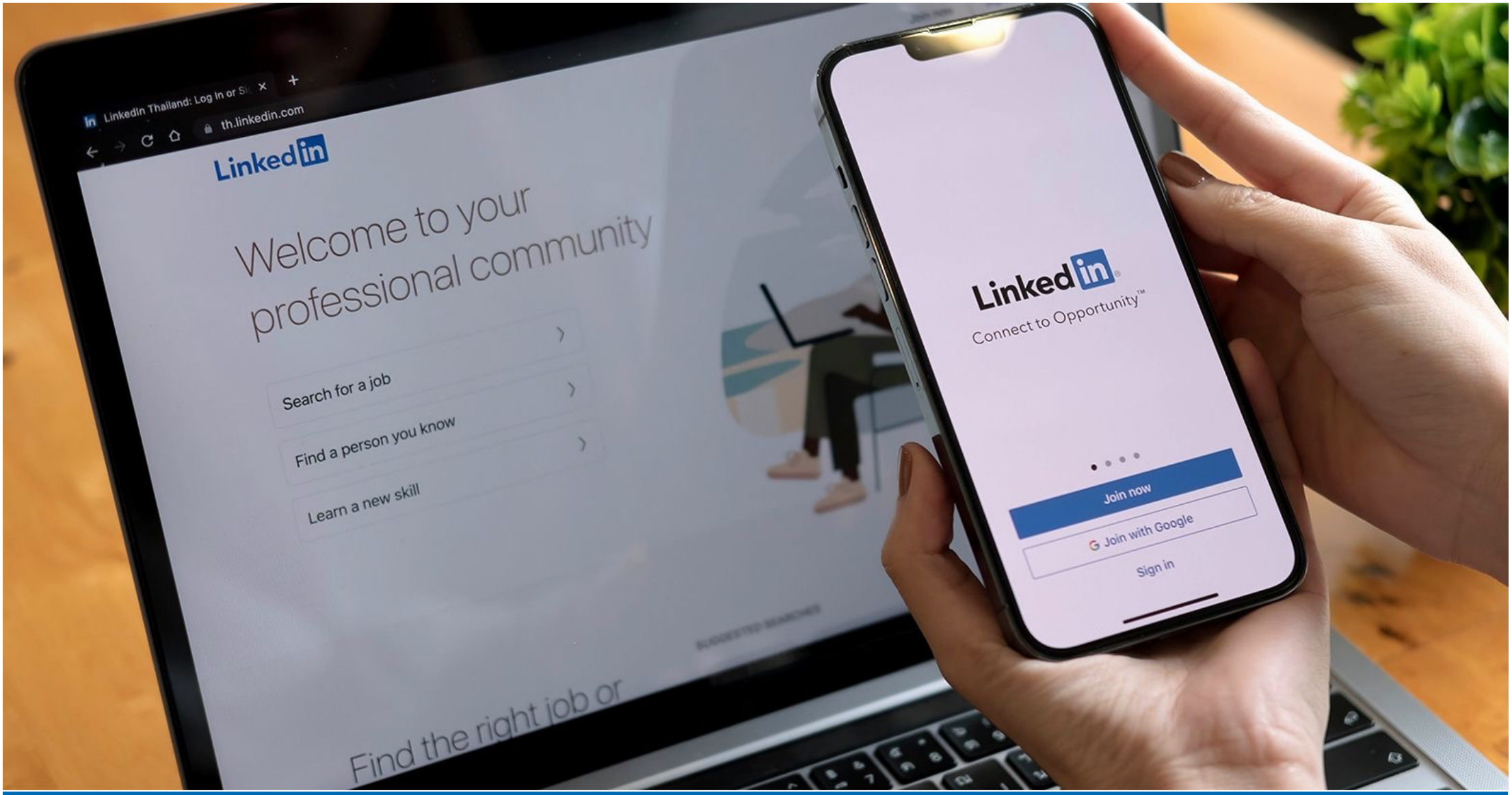
N’utilisez PAS votre vrai nom d’utilisateur
N’utilisez PAS votre vrai mot de passe

Linked in

Faked in

Only works during the presentation

https://sncb.cybersteven.be:8090


LinkedIn Thailand: Log In or Si
th.linkedin.com
LinkedIn
Welcome to your professional community
Search for a job
Find a person you know
Learn a new skill
Find the right job or
LinkedIn
Connect to Opportunity™
Join now
Join with Google
Sign in

Conclusion : Ton comportement = la cybersécurité

Les hackers n’ont pas besoin de pénétrer votre serveur.
Ils cherchent à pénétrer votre esprit.

Avec la bonne formation, l’utilisateur cesse d’être le maillon faible et devient la meilleure défense.

Merci pour votre attention

Steven Debruyn

https://www.linkedin.com/in/stevendebruyn