Project n° 101083886 Dihnamic

Cofinancé par l'Union européenne

RÉGION Nouvelle-Aquitaine

dihnamic

Cybersécurité
Et si l'on s'intéressait à l'humain ?

Webinaire du 28/04/23

Dihnamic, c'est quoi ?

Le but de Dihnamic est de favoriser l'appropriation des technologies numériques avancées par les entreprises manufacturières et les autorités publiques de la Nouvelle-Aquitaine.

4 Nœuds d'innovation :

- Intelligence artificielle
- Robotique, process agiles et Interface Homme-Machine
- Jumeaux Numériques
- Systèmes intelligents et internet des objets

Cofinancé par l'Union européenne

Dihnamic : 13 partenaires

adi nouvelle-aquitaine
Agence de développement et d'innovation

aerospace valley

ALPHA RLH
ROUTE DES LASERS & DES HYPERFREQUENCES

BORDEAUX INP

CAP'TRONIC

CATIE
Solutions pour la société numérique

cea

cetim

cetim Sud-Ouest

eit Manufacturing
CLC WEST

Co-funded by the European Union

ESTIA
INSTITUTE OF TECHNOLOGY
une école
CCI BAYONNE PAYS BASQUE
Euskal Herri

Inria

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ONERA
THE FRENCH AEROSPACE LAB

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Partenaires associés :

Agri Sud-Ouest Innovation | Cosmetic Valley | École Nationale Supérieure d'Arts et Métiers (campus Bordeaux-Talence) | Metallicadour | Pôle Européen de la Céramique | Université de Bordeaux

Cofinancé par :

Cofinancé par l'Union européenne

RÉGION Nouvelle-Aquitaine

Votre accompagnement au sein de Dihnamic : proximité et personnalisation

CONTACTEZ NOUS
Un contact personnalisé

EVALUATION PERSONNALISEE GRATUITE
de votre maturité digitale
Un diagnostic Dihnamic
Porté par des experts,
De proximité (en présentiel, au sein de votre structure)

PRECONISATIONS
Un bilan confidentiel qui vous est livré,
assorti de préconisations (proposition de services),
que vous choisirez ou non de mettre en œuvre avec notre support

DEPLOIEMENT DE SERVICES

EVALUATION A L'ISSUE DU SERVICE :
Impact au sein de votre structure

SATISFACTION

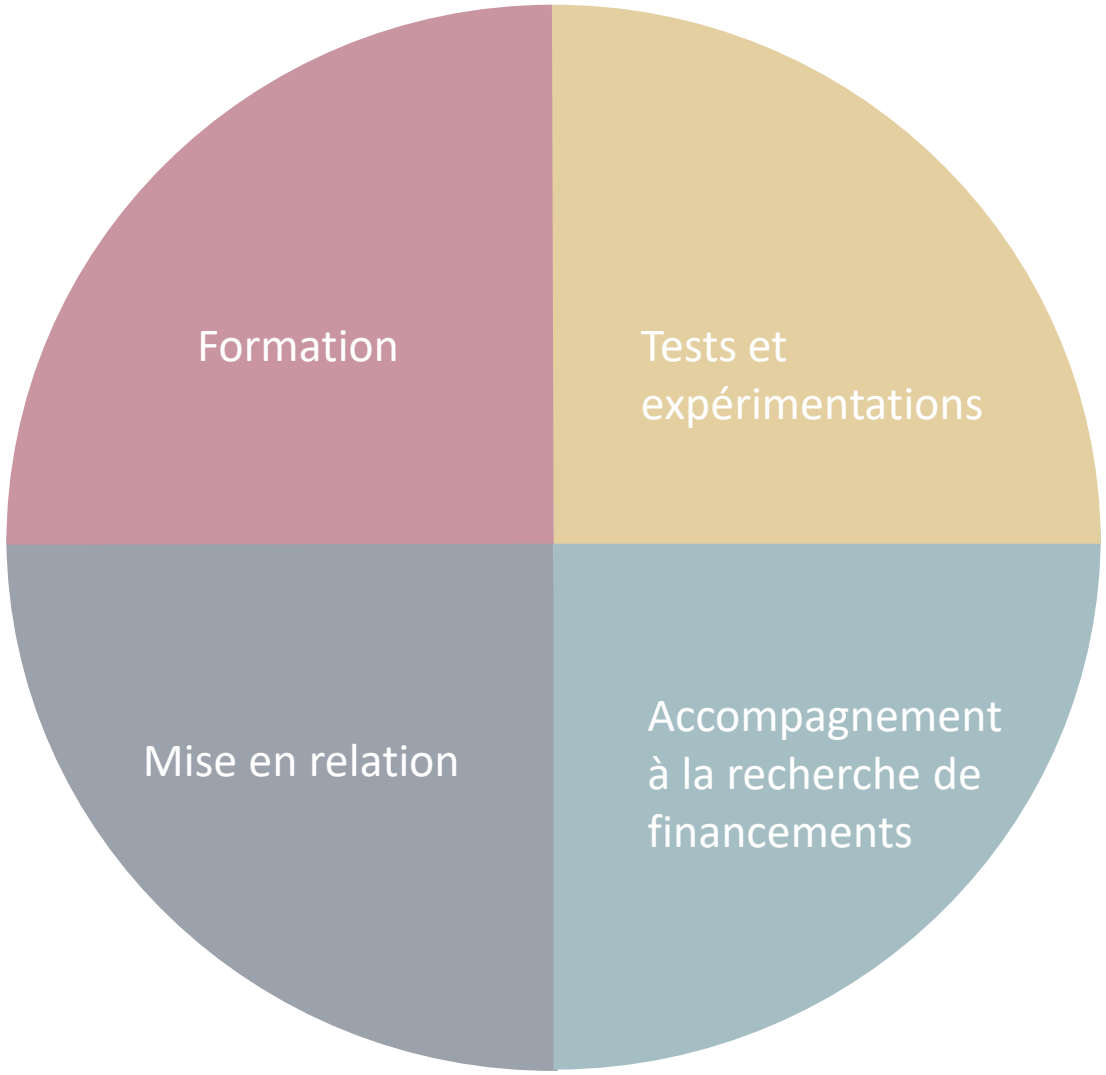
AUTRES ACTEURS DE L'ECOSYSTEME POUR COMPLETER LA TRANSFORMATION NUMERIQUE

PRECONISATIONS : AUTRES SERVICES Dihnamic

Votre parcours suivi par un comité d'excellence

Cofinancé par l'Union européenne

Les services de Dihnamic : de la preuve de concept à la recherche de financement



Des services complémentaires, à la carte en fonction des besoins identifiés lors de la phase d'analyse et de diagnostic.

Des acteurs de haut niveau (centre techniques, universitaires, pôles) pour des services innovants avec une haute valeur ajoutée.

Cofinancé par l'Union européenne

Présentation

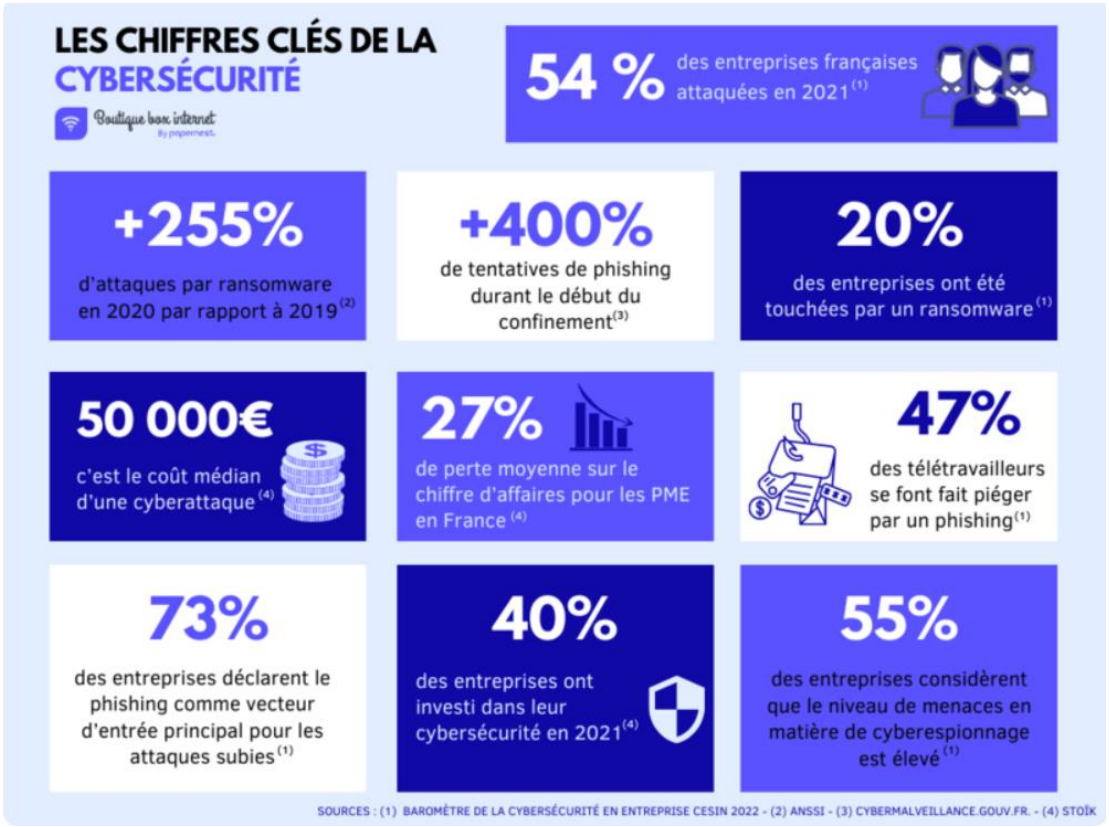
- Ingénieur Recherche & Développement dans le domaine des Facteurs Humains au CATIE depuis 8 ans.
- Spécialisation dans l'analyse des données comportementales et physiologiques du pôle Systèmes Centrés sur l'Humain.
- Auparavant, statisticien dans la banque pendant 20 ans

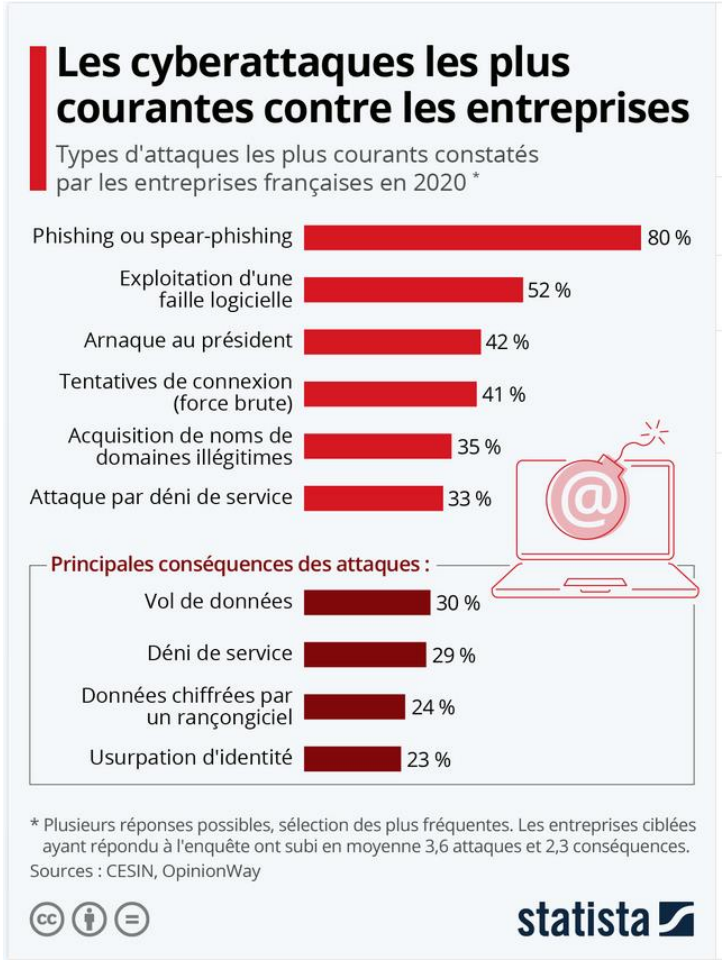
Sommaire

- Quelques chiffres clefs de la cybersécurité
- Cybersécurité : Les comportements à risque
- L'ingénierie sociale
- Le modèle de persuasion ELM
- Les principaux facteurs explicatifs de vulnérabilité
- Les recommandations/actions
- Bibliographie

Cofinancé par l'Union européenne

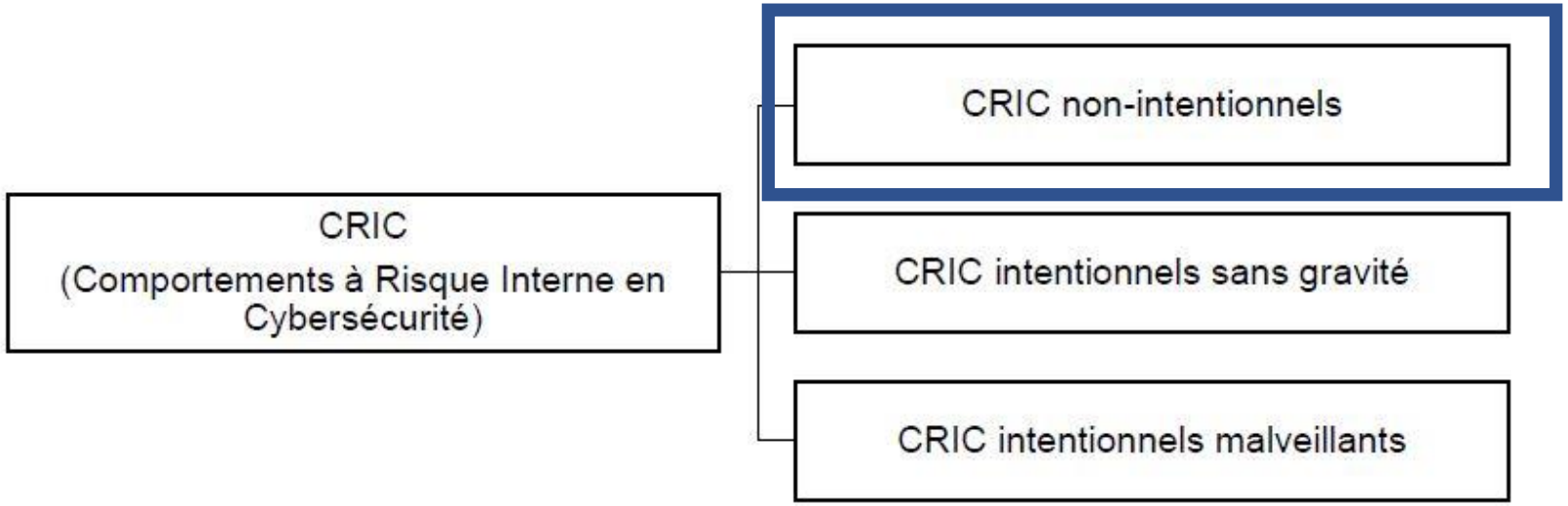
Cybersécurité et FH : Les enjeux





Cybersécurité et FH : Les comportements à risque

Dans une organisation : 3 sous-catégories de risques



Classification des Comportements à Risques Internes en Cybersécurité - J. Le Roy (2021)

L’ingénierie sociale : Définitions

- Cyberattaque par ingénierie Sociale : type d’attaques informatiques qui exploitent les failles et les faiblesses psychologiques humaines en tentant de persuader un individu (une victime) à agir comme prévu, selon un scénario malicieux et efficace à la fois
- Quelques formes d’ingénierie sociale :
  - Phishing ou hameçonnage
  - Spams,
  - Spear phishing,
  - Utilisation de « sock puppets » sur les réseaux sociaux.,
  - Fraudes,
  - Ingénierie sociale inversée,
  - …

L’ingénierie sociale : Contexte

- Prélude souvent à des cyberattaques beaucoup plus sophistiquées et dévastatrices.
- Recherches en ingénierie sociale principale basées sur la compréhension et/ou la détection des attaques d’un point de vue technologique. Composantes psychologiques de ces attaques peu abordées
- Le succès des cyberattaques d’ingénierie sociale est inversement lié à leur prévalence. Lorsque les défenses automatisées sont efficaces pour détecter et filtrer la plupart des cyberattaques d’ingénierie sociale, les attaques restantes ont plus de chances d’aboutir.
- Difficultés éthiques et de représentativité des populations étudiées

L'ingénierie sociale : Les stratégies d'attaque

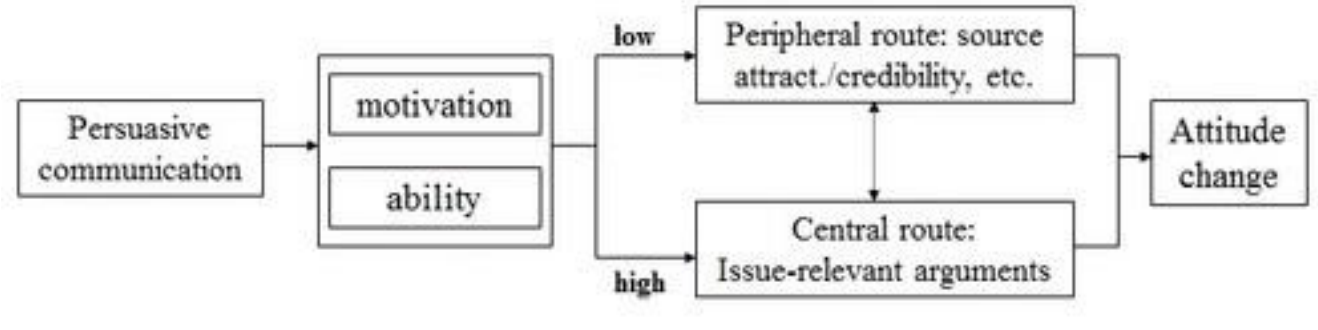
- Les stratégies de détournement amygdalien

Appellation	Définition	Exemple
Aimer	Génère un faux sentiment de crédibilité	Les cybercriminels peuvent l'utiliser pour établir des relations ou encourager certains comportements en générant de faux likes et en augmentant artificiellement le nombre de followers sur les réseaux sociaux pour donner l'impression que d'autres personnes soutiennent ce comportement.
Réciprocité	Provoque un sentiment d'obligation de rendre des faveurs	Les cybercriminels peuvent offrir des services ou des produits gratuits et s'attendre à un accès ou à des données en retour.
Preuve sociale ou le consensus	Facilite le soutien et l'engagement dans les attitudes d'autrui	Les cybercriminels peuvent utiliser ce type de validation pour influencer les utilisateurs et accéder aux données. Lorsque les utilisateurs ne sont pas certains, ils peuvent facilement répondre à d'autres personnes, en particulier à leurs pairs.
Persuasion par les pairs	Persuasion par les pairs	Les cybercriminels peuvent persuader des initiés de voler des données pour une cause qu'un pair ou un modèle de rôle promeut.
Autorité	Abus de pouvoir de l'autorité	L'autorité peut apporter de fausses réclamations et influencer un utilisateur qui se méfie de la perte d'emploi.
Cohérence.	S'appuie sur le besoin d'apparaître ou de rester cohérent	Les cybercriminels peuvent découvrir des actions cohérentes et les utiliser pour distraire un utilisateur avant une attaque.
Rareté des ressources	Rend un utilisateur vulnérable	Il peut inciter un utilisateur à prendre une action immédiate sans penser aux conséquences telles qu'une violation de données.

7 principales stratégies d'ingénierie sociale (J. Le Roy,2021)

Le modèle ELM de persuasion

Modèle de probabilité d'élaboration (ELM) de Petty et Cacioppo (1986)



- 2 types de traitement de l'information : Central (implication forte) et périphérique (implication faible)
- Les routes impliquent des différences de traitement de l'information en terme d'attention et d'élaboration

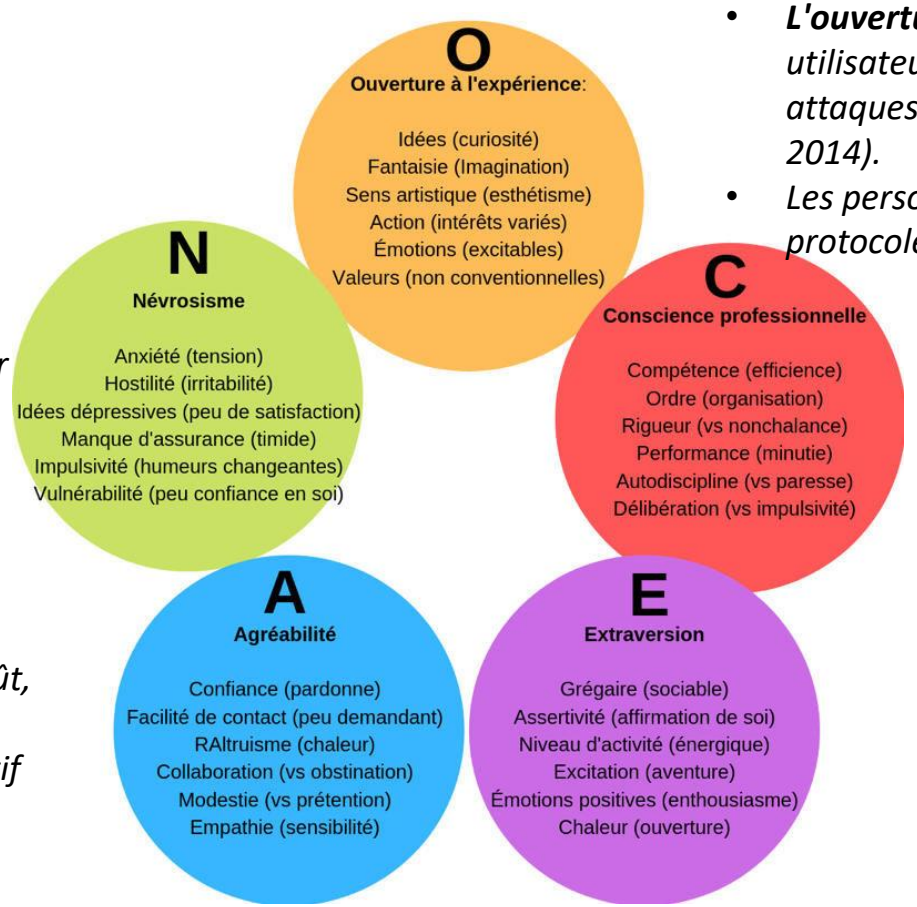
Les Facteurs de vulnérabilité

Facteurs cognitifs court-terme

- La **charge cognitive** peut réduire considérablement la capacité d'un utilisateur à détecter les indices malveillants. Par exemple, lorsque les e-mails malveillants coïncident avec un volume d'e-mails élevé (van der Heijden et Allodi, 2019)
- Le **stress aigu** peut influencer l'attention de manière aussi bien bénéfique que préjudiciable (Al'Absi et al., 2002).
  - L'effet tunnel attentionnel : Attention focalisée sur les aspects pertinents à cause du stress, mais moins sensible aux autres informations. Exemple : prêter attention au texte d'un mail et ignorer des indices périphériques comme une adresse mail suspecte
  - Le stress peut dans certain cas altérer la prise de décision rationnelle.
- Purkait et al. (2012) ont trouvé des associations positives entre la détection de l'hameçonnage et des mesures expérimentales de la **vigilance** et de la **mémoire à court terme**.

Les Facteurs de vulnérabilité

La personnalité
Exemple du Big 5



*Le **névrosisme** indique qu'un utilisateur est moins sensible à la plupart des attaques d'ingénierie sociale (Jin-Hee Cho et al.,2016)*

***Agréabilité** : vulnérabilité envers le goût, l'autorité, la réciprocité et la preuve sociale (J. Le Roy, 2021). Effet significatif sur la confiance, le risque perçus, et la performance des décisions (Jin-Hee Cho et al.,2016)*

- ***L'ouverture** réduit la vulnérabilité de l'ingénierie sociale car les utilisateurs plus éduqués au numérique détectent mieux les attaques d'ingénierie sociale (Caulkins 2017; Uebelacker et Quiel 2014).*
- *Les personnes **ouvertes** sont plus susceptibles de violer un protocole de cybersécurité (McBride et al., 2012)*

- *Les individus **moins impulsifs** gèrent mieux les messages de phishing. (Darwish et al., 2012; Pattinson et al, 2012).*
- *Un utilisateur **consciencieux** peut ne pas résister aux principes d'autorité, de réciprocité, d'engagement et de cohérence, en particulier lorsque les engagements sont rendus publics (J. Le Roy , 2021)*

*Selon Lawson et al. 2018), **l'extraversion** diminue la précision de la détection du phishing.* L'utilisateur **d'extraversion** peut être plus vulnérable au principe de rareté (excitation)

*Darwich et al. (2012) constatent que les individus plutôt **extravertis** et dotés **d'amabilité**, posent un risque plus élevé pour la sécurité informatique.*

Les Facteurs de vulnérabilité

L’expérience et la connaissance

- Harrison et al. (2016) constatent que **les connaissances sur les attaques de phishing** augmentent l’attention et l’élaboration lorsqu’elles sont **combinées à une expérience subjective** ; elles réduisent donc la susceptibilité d’être victime de messages de cyberattaque par ingénierie sociale.
- Wright et Marett (2010) ont constaté que les **connaissances en matière de sécurité et l'expérience du web** rendaient les utilisateurs moins susceptibles d'être trompés.
- l'effet d'interaction des **connaissances conceptuelles et procédurales a un impact positif sur l'auto-efficacité** des utilisateurs d'ordinateurs, ce qui renforce leur comportement d'évitement de la menace du phishing (Arachchilage & Love, 2014).
- ⚠ L’expertise n’est pas transférable d’un domaine à une autre. Risque d’excès de confiance

Les Facteurs de vulnérabilité

Des variabilités démographiques

- Abbasi et al. (2016) constatent que les femmes et les hommes plus âgés et instruits qui ont été victimes d'attaques de phishing dans le passé sont moins susceptibles d'être à nouveau victimes d'attaques de phishing
- Gavett et al., 2017 mettent en avant l'effet principal des **années d'éducation** ainsi que la combinaison entre l'**âge** et la **connaissance préalable** de l'hameçonnage. Les jeunes adultes (18-25 ans *vs* +25 ans) ont une probabilité plus forte d'être victime de hameçonnage (Darwich et al., 2012).
- En revanche, l'étude de Halevi et al., 2017 montre que **les différences culturelles** des individus n'affectent pas de manière significative leur comportement en matière de cybersécurité et d'auto-efficacité dans la gestion des menaces.

Les Recommandations/actions

Thème	Recommandation
Sensibilisation	Aider à expliquer la nécessité pour l'internaute de se protéger ou d'éviter les comportements à risque lorsqu'il effectue des transactions financières sur Internet.
Efficacité de la formation	Prédire dans une organisation quels profils de personnalité sont plus exposés à l'ingénierie sociale, suggérant ainsi des scénarios personnalisés de formation à la cybersécurité.
	Formation mixant enseignement des connaissances conceptuelles et des connaissances procédurales (impact positif sur l'auto-efficacité des utilisateurs)
	Se concentrer davantage sur l'amélioration de la qualité de l'attention initiale portée au courrier électronique. Cela peut être amélioré en apprenant aux utilisateurs à prêter attention à quelques éléments clés du message.
	Former les salariés à la compréhension des mécanismes psychologiques qui structurent et sous-tendent notre exposition et notre vulnérabilité aux cyberattaques.

Thème	Recommandation
Outils de formation	Développer un outil dans laquelle les utilisateurs jouent un rôle dans une boîte de réception de courrier électronique simulée et se voient présenter plusieurs scénarios différents. Les participants sont exposés à plusieurs types d'hameçonnage par courrier électronique et peuvent expérimenter les résultats des réponses appropriées et inappropriées. → Education par l'expérience et amélioration de l'efficacité personnelle
Adaptation des outils de sécurité	Développer des outils de sécurité personnalisés pour les employés en fonction de plusieurs caractéristiques personnelles.
	Fournir des recommandations pragmatiques pour développer des interventions centrées sur l'utilisateur afin de contrecarrer les attaques de phishing
Perception de l'outils de détection de hameçonnage	L'amélioration des perceptions des utilisateurs concernant l'utilité des outils de détection d'hameçonnage doit être un point central

DES QUESTIONS ?

- Contact : f.potier@catie.fr

MERCI POUR VOTRE ATTENTION

Bibliographie

- Abbasi, A., Zahedi, F. M., & Chen, Y. (2016). Phishing susceptibility : The good, the bad, and the ugly. *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 169-174. https://doi.org/10.1109/ISI.2016.7745462
- Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). COVID-19 and Phishing : Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic. *IEEE Access*, *9*, 121916-121929. https://doi.org/10.1109/ACCESS.2021.3109091
- Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users : A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312. https://doi.org/10.1016/j.chb.2014.05.046
- Darwish, A., Zarka, A. E., & Aloul, F. (2012). Towards understanding phishing victims' profile. *2012 International Conference on Computer Systems and Industrial Informatics*, 1-5. https://doi.org/10.1109/ICCSII.2012.6454454
- Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. *Proceedings of the Second Symposium on Usable Privacy and Security - SOUPS '06*, 79. https://doi.org/10.1145/1143120.1143131
- Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults : The role of executive functioning. *PLOS ONE*, *12*(2), e0171620. https://doi.org/10.1371/journal.pone.0171620
- Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks : Phishing attack. *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 537-540. https://doi.org/10.1109/CCAA.2016.7813778
- Halevi, T., Memon, N., & Nov, O. (2015). Spear-Phishing in the Wild : A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2544742
- Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails : How attention and elaboration protect against phishing. Online Information Review, 40(2), 265-281. https://doi.org/10.1108/OIR-04-2015-0106

Bibliographie

- Rodriguez, R. M., Golob, E., & Xu, S. (2020). *Human Cognition through the Lens of Social Engineering Cyberattacks* (arXiv:2007.04932). arXiv. http://arxiv.org/abs/2007.04932
- de Barnier, V. (2006). Le modèle ELM : Bilan et perspectives. *Recherche et Applications en Marketing (French Edition)*, *21*(2), 61-82. https://doi.org/10.1177/076737010602100204
- Roy, J. L. (2021). *Psyber Sécurité : L'apport de la psychologie dans le management de la cybersécurité*. 21.
- Jin-Hee Cho, Hasan Cam, & Oltramari, A. (2016). Effect of personality traits on trust and risk to phishing vulnerability : Modeling and analysis. 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA),
- Redmiles, E. M., Chachra, N., & Waismeyer, B. (2018). Examining the Demand for Spam : Who Clicks? Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 1-10. https://doi.org/10.1145/3173574.3173786
- Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility. *Communication Research*, *45*(8), 1146-1166. https://doi.org/10.1177/0093650215627483
- Teboul, D. B. (2021). Approche cognitive des cyberattaques par ingénierie sociale. *The European Scientist*, 14.