Jean-Marie VIGNEAUD

Fraude au Président : exploiter les traits de personnalité des personnes ciblées pour réduire la réponse aux attaques

Promotion 2024-2025

RESUME

En 2023, les faux ordres de virement ont constitué la menace de cybercriminalité en plus forte progression, notamment via la fraude au Président. Ce type de fraude repose sur l'usurpation de l'identité de cadres dirigeants (président, directeur financier…) par l'envoi de courriels de spear phishing, incitant des collaborateurs à exécuter des virements sous pression psychologique, souvent au nom d'une urgence ou d'un dossier confidentiel. Les services comptables, RH et de paie, disposant d'un accès privilégié à des informations sensibles et à des moyens de paiement, constituent des cibles privilégiées.

Ces attaques exploitent des biais cognitifs (biais d'autorité, biais d'ancrage, etc.) et jouent sur des émotions telles que l'urgence ou la peur, afin de limiter la capacité de la victime à évaluer l'authenticité de la requête.
Des recherches récentes indiquent que la « susceptibilité au phishing » est influencée par certains traits de personnalité. À ce titre, une étude exploratoire est envisagée afin d'examiner la relation entre ces traits, identifiés à travers le modèle des « Big Five », et la propension des individus à céder à des tentatives de fraude au Président.

Deux hypothèses principales guident cette démarche :

- Certains traits de personnalité, identifiés par le modèle Big Five, accentueraient la vulnérabilité aux attaques de type fraude au Président, en raison de leur résonance avec les ressorts psychologiques mobilisés par les attaquants.
- Une sensibilisation ciblée, fondée sur les résultats individuels de ces tests, permettrait de renforcer la vigilance des personnels des services financiers et de réduire significativement les risques liés à ces fraudes.

1 - INTRODUCTION

Au cours de l'année 2023, les principales menaces en matière de cybercriminalité qui ont le plus augmenté sont les faux ordres de virement (+63 %) [1]. Elles peuvent se traduire de différentes façons, dont une des plus connu est la fraude au Président. Dans ce cas d'espèce, l'escroc usurpe l'identité du Président, du Directeur financier ou d'un ordonnateur au travers d'un envoi de mail, et demande par exemple à un collaborateur d'effectuer un virement de toute urgence à un tiers, au prétexte d'un dossier sensible et confidentiel, par exemple. Ces attaques se caractérisent par l'utilisation de communications bien préparées et authentifiées, qui imitent des messages légitimes provenant de sources de confiance au travers de mails de spear phishing.

Les services comptables, de paie ou RH des entreprises sont des cibles privilégiées pour ces types d'attaques, en raison du fait qu'ils ont accès à des informations sensibles et qu'ils peuvent opérer des transactions financières.

Pour arriver à leurs fins, les attaquants utilisent des leviers psychologiques [2] tels que des biais cognitifs (biais d'autorité, biais d'ancrage, …), et manipulent les émotions de leur cible en jouant sur les sentiments d'urgence ou de peur, incitant les individus à agir rapidement sans procéder à des vérifications approfondies de l'authenticité de la communication.

Des études récentes ont montré que la caractéristique appelée « susceptibilité au phishing » est étroitement liée aux traits de personnalité des individus [3] qui jouent un rôle crucial dans notre sensibilité aux attaques, lesquelles sont souvent qualifiées d'attaques psychologiques [4].

Dans ce contexte, nous nous proposons de mener une étude exploratoire en exploitant le test de personnalité « Big 5 », utilisé par les entreprises lors des recrutements pour identifier les traits saillants des candidats. Nous nous interrogerons sur la corrélation qu'il peut y avoir entre certains de ces traits et la propension à donner suite à des tentatives de fraude au Président.

Nous ferons ici deux hypothèses :

H1 : Le test Big 5 permet de mettre en évidence des traits de personnalités spécifiques susceptibles d'augmenter la sensibilité aux attaques de type fraude au Président, faisant notamment écho aux leviers psychologiques utilisés par les attaquants lors de telles opérations.

H2 : La mise en place d'actions ciblées au sein des services financiers, utilisant les résultats de ces tests individuels, permet d'améliorer la vigilance des collaborateurs de façon significative, en leur faisant prendre conscience de leurs fragilités intrinsèques.

Pour ce faire, après avoir décrit les mécanismes psychologiques utilisés par les hackers dans un contexte de fraude au Président, nous décrirons au travers de la littérature existante l'apport des tests de personnalités et nous extrapolerons la corrélation qu'il peut exister entre certains traits et le comportement des individus face à de telles attaques. Nous illustrerons le propos par des cas d'attaques réelles survenues récemment au sein de la Safer Nouvelle-Aquitaine, et définirons les actions à mettre en place pour prévenir de futures attaques.

2. FRAUDE AU PRÉSIDENT – LEVIERS PSYCHOLOGIQUES UTILISÉS

L'une des principales forces des cybercriminels ne réside pas seulement dans l'utilisation de malwares de haute technologie, mais dans l'exploitation de la vulnérabilité de l'esprit humain. Les attaques d'ingénierie sociale, comme la fraude au Président, tirent parti de mécanismes psychologiques tels que la confiance, la peur, l'urgence ou les biais cognitifs [5]. Un rapport récent de Verizon [6] révèle que 68 % des violations de données impliquent un facteur humain.

Ces attaques reposent sur la technique dite du spear phishing qui se distingue comme une forme particulièrement ciblée et sophistiquée de phishing. Contrairement aux attaques de phishing classiques, qui visent un large public, elles s'attaquent spécifiquement à des individus occupant le plus souvent des postes à responsabilité [7].

Ces attaques se caractérisent par l'utilisation de communications bien préparées et authentifiées qui imitent des messages légitimes provenant de sources de confiance et qui incitent les collaborateurs à exécuter des actions, souvent liées à des transactions financières.

Pour arriver à leurs fins, les hackers exploitent plusieurs biais cognitifs [8] qui jouent sur les vulnérabilités psychologiques des victimes, en particulier celles qui se trouvent dans des positions de responsabilité ou qui sont soumises à une certaine pression.

Le principal biais utilisé dans ce type d'attaque est le biais d'autorité [9]**.** Les hackers se font souvent passer pour une figure d'autorité, comme le Président, un Directeur financier, ou un autre responsable de l'entreprise ciblée. En usurpant cette identité, ils exploitent la tendance humaine à faire confiance à l'autorité sans se poser de question, en particulier dans des environnements hiérarchiques élevés . Les employés, face à une demande perçue comme émanant de leur supérieur, obéissent généralement sans vérifier les informations, comme a pu le démontrer Milgram dans sa théorie concernant l'autorité et l'obéissance [10].

Le biais de l'ancrage [11] survient, quant à lui, lorsque les individus prennent des décisions en s'appuyant excessivement sur la première information qu'ils reçoivent. Dans le cadre de la fraude au Président, un hacker peut envoyer un e-mail en prenant comme point de départ une information familière (comme une référence à une transaction courante), et l'ancrer dans l'esprit de la victime. Cela la rend moins susceptible de remettre en question la demande de virement, surtout si elle est dans une situation de stress ou de confusion.

Enfin, un autre biais utilisé dans ce type d'attaque est le biais de familiarité [12], qui se traduit par l'inclination à considérer comme plus sûr, crédible ou fiable tout ce qui est familier. Dans le domaine de la cybersécurité, cela signifie que les messages ou les requêtes ressemblant à des communications internes, déjà vues ou auxquelles l'individu est habitué, sont moins susceptibles d'être remis en question. La reproduction d'éléments visuels et linguistiques (logos, signatures, mise en page, et même le style rédactionnel habituel) crée un sentiment de familiarité qui incite la victime à baisser sa garde. De même, l'utilisation de canaux de communication connus (adresse e-mail interne par exemple) renforce la crédibilité du message frauduleux. Enfin, la personnalisation des messages (noms, projets en cours, événements internes) rend le message encore plus familier et renforce sa véracité.

De plus, au-delà de l'exploitation des biais cognitifs, les hackers utilisent d'autres stratégies qui leur permettent de mettre l'utilisateur dans des postures psychologiques spécifiques en créant un sentiment d'urgence ou de peur [13].

Pour illustrer nos propos, nous présentons ici un e-mail issu d'une campagne de fraude au Président lancée en janvier 2025 contre le service RH de la SAFER Nouvelle-Aquitaine concernant une tentative de fraude au virement de salaire sur un faux RIB. Des e-mails similaires ont été envoyés à différents collaborateurs en charge de la paie, avec une formulation et des signataires différents. Le seul objectif de cette campagne est de détourner des virements de salaires en invoquant un changement de situation bancaire.

Bonjour Martine

Je t'envoie ce mail car je souhaite mettre à jour mes informations bancaires avant la prochaine paie. De quels détails auriez-tu besoin ?
Peux-tu m'aider à faire cette mise à jour le plus tôt ? Je reste à disposition pour toutes informations complémentaires

Cordialement
Edouard B[redacted]
Responsable du Service régional Environnement et Collectivités
Safer Nouvelle-Aquitaine

Nous pouvons retrouver dans cet e-mail tous les éléments caractéristiques de la fraude au Président.

Le fait de commencer le message par le prénom de la personne en charge des RH, suivi d'un style où le tutoiement domine, favorise ainsi une certaine proximité et une communication plutôt informelle ou amicale. Cela diminue la vigilance et rend la cible plus susceptible de répondre à la demande.

La notion d'urgence de la situation est ici largement utilisée : *« avant la prochaine paie »*, *« faire la mise à jour au plus tôt »*.

La formule *« Peux-tu m'aider … »,* provenant d'un collègue, incite à rendre service.

Enfin, la personne qui signe cet e-mail a un niveau hiérarchique élevé, favorisant ainsi le biais d'autorité.

Comme nous pouvons le constater au travers de cet exemple très simple, ces cyberattaques sont assez sophistiquées et font appel à de nombreux leviers psychologiques. Les chercheurs ont étudié différents aspects des traits et comportements humains pour comprendre ce qui augmente la vulnérabilité au

phishing. L'impact des traits de personnalité sur la vulnérabilité au phishing, notamment mesuré à l'aide du modèle des Big 5, a été abordé dans plusieurs articles [14] [15] [16].

3. LE TEST DE PERSONNALITÉ BIG 5

Pour les psychologues [14], la personnalité fait référence aux différences individuelles affectant les pensées, les sentiments et les comportements qui sont cohérents dans le temps (même s'ils peuvent évoluer, avec l'âge notamment). Des modèles permettent de décrire les traits de personnalité d'un individu. Chaque personne peut présenter un niveau faible, moyen ou élevé pour chacun de ces traits, dessinant ainsi un profil bien spécifique.

La recherche sur la personnalité est dominée par le cadre des « Big 5 » des domaines de la personnalité, qui a été développé pendant une grande partie du XX^{e} siècle sous diverses formes [14]. Il a été démontré [17] que ces traits sont stables dans le temps et universellement identifiables indépendamment de la langue, de la race, de la culture ou du sexe. Ces dimensions sont en effet considérées comme étant les traits sous-jacents qui composent la personnalité globale d'un individu.

Considéré par de nombreux cabinets de recrutement comme le modèle le plus fiable et le plus riche en enseignements, le modèle Big 5 est également celui qui fait consensus, aujourd'hui, au sein de la communauté scientifique. Il a fait l'objet de nombreuses recherches qui ont confirmé sa validité et sa robustesse [18] [19] [20]. Il découle en effet d'observations et d'analyses statistiques validées scientifiquement. Le modèle du Big 5 (parfois appelé FFM – Five Factor Model) est le plus utilisé en psychologie universitaire. Décliné sous divers formats de questionnaires, le modèle français est composé de 45 items accompagnés d'une échelle de Likert en cinq niveaux : de 1 (désapprouve fortement) à 5 (approuve fortement).

Le framework Big 5 définit cinq grandes dimensions de la personnalité qui sont :

a) **L'ouverture à l'expérience** (**O**penness) :

↗ Les personnes qui obtiennent un résultat élevé se distinguent par leur caractère non conventionnel, créatif, intellectuel, curieux, et par leur imagination débordante. Elles aiment entendre des opinions nouvelles et inhabituelles.

↘ Les personnes obtenant un résultat faible sont conventionnelles, traditionnelles et n'apprécient pas les choses étrangères et qu'elles connaissent mal. Les activités intellectuelles les laissent de marbre et elles n'aiment pas être confrontées à des opinions et à des idées bizarres.

b) **La conscienciosité** (**C**onscientiousness**)** :

↗ Les personnes qui obtiennent un résultat élevé sont bien organisées, travailleuses, disciplinées, efficaces, consciencieuses et ordonnées dans leur rapport aux choses et au temps.

↘ Les personnes possédant des résultats faibles sont distraites, désordonnées, ont du mal à trouver la motivation nécessaire à accomplir leur travail et leurs devoirs, ne sont pas gênées par l'inachèvement et le manque d'exactitude, et sont désorganisées en ce qui concerne leur environnement et leur emploi du temps.

c) **L'extraversion (E**xtraversion**) :**

↗ Les personnes qui obtiennent un résultat élevé sont extraverties, vives, sociables, bavardes, sûres d'elles, joyeuses, et apprécient les interactions sociales.

↘Les personnes obtenant un résultat faible sont réservées, calmes, effacées et moins dépendantes de la vie sociale

d) **L'agréabilité (A**greeableness**)** :

↗ Les personnes qui obtiennent un score élevé sont tolérantes, douces, gentilles, indulgentes, agréables, altruistes et obligeantes. Comme il est très important pour elles de bien s'entendre avec les autres, elles ont des opinions flexibles et répugnent à critiquer ou à juger.

↘ Les personnes dont l'agréabilité est faible sont sceptiques, têtues, querelleuses, intéressées et brusques. Les personnes dont l'agréabilité est faible ont aussi tendance à défendre bec et ongles leurs avis et leurs opinions, et à critiquer les autres. L'agréabilité n'est pas toujours utile dans les situations qui demandent de prendre des décisions difficiles ou objectives. Des études ont montré qu'un faible degré d'agréabilité peut avoir de nombreux avantages pour les leaders et les avocats.

e) **Le névrosisme (N**euroticism**)** :

↗ Les personnes qui obtiennent un résultat élevé sont inquiètes, anxieuses, dépressives, complexées et vulnérables au stress et à la dépression.

↘ Les personnes qui obtiennent un résultat faible sont calmes, stables, sereines et peu sujettes à l'angoisse. Elles surmontent facilement la colère, le stress et la gêne. Un résultat faible en névrosisme semble donc être une situation enviable, mais, cependant, les personnes qui obtiennent un faible résultat peuvent aussi se révéler trop insouciantes et trop enclines à sous-estimer les menaces potentielles de leur environnement.

Ces 5 traits de personnalité forment l'acronyme O.C.E.A.N.

Des recherches ont montré que ces traits sont indépendants les uns des autres. Une personne ayant un niveau élevé d'ouverture à l'expérience (O) ne présume en rien de son degré d'extraversion (E), ni de sa gentillesse (A) ou de sa stabilité émotionnelle (N) par exemple [21].

Nous allons maintenant décrire, à la lumière de la littérature existante, comment chacun de ces traits de personnalité peut jouer en faveur/défaveur des attaquants et des biais qu'ils peuvent exploiter, en s'appuyant sur plusieurs études récentes.

4 – TRAITS DE PERSONNALITÉ ET SENSIBILITÉ AU PHISHING

Un vrai changement de paradigme s'opère par la réorientation de l'analyse des failles et des vulnérabilités « *techno-centrées* », vers le prisme d'une analyse « neurocognitive » : où les faiblesses de l'esprit humain sont démontrées, diagnostiquées et mises à l'épreuve par des tests psychologiques qui nous indiquent, pourquoi et comment les humains sont vulnérables et peuvent à tout moment cliquer sur un lien malveillant et déclencher une catastrophe en chaîne [4].

Tout d'abord, la relation entre la personnalité Big 5 et le principe de persuasion sont discutés dans la littérature [22] concernant l'analyse de la susceptibilité au phishing. La théorie du « Social Engineering Personality Framework » a été proposée, et l'influence des traits de personnalité des Big 5 sur la susceptibilité au phishing a été expliquée sur la base de recherches antérieures. Les conclusions suivantes, souvent discutées, ont été tirées.

L'ouverture à l'expérience, ou l'intérêt pour l'innovation, se caractérise par une curiosité intellectuelle et une volonté d'explorer de nouvelles idées et expériences. Cela peut avoir des effets variés sur la vulnérabilité au phishing. Les connaissances techniques et les compétences informatiques liées à l'ouverture ont contribué à une moindre vulnérabilité [14]. Mais d'autres études constatent que les personnes ayant un haut degré d'ouverture sont plus enclines à la curiosité et peuvent potentiellement cliquer sur des liens et ouvrir des fichiers intéressants ou intrigants, sans vérifier leur sécurité [23] [24].

La conscienciosité, qui est associée à la rigueur, à l'organisation et à l'autodiscipline, est probablement l'un des traits les plus protecteurs face au phishing. En effet, les personnes très consciencieuses sont généralement plus attentives aux détails et plus susceptibles de vérifier la légitimité d'un message avant d'agir. Leur tendance à éviter les risques et à suivre les règles les rend moins enclines à cliquer sur des liens suspects ou à fournir des informations personnelles [25]. Une autre étude a révélé que de faibles niveaux de conscience étaient associés à des comportements déviants sur le lieu de travail, tels que la violation des règles ou un comportement irresponsable, et étaient donc plus susceptibles de cliquer sur un lien en dépit des consignes de sécurité [14].

L'extraversion, caractérisée par une tendance à rechercher des interactions sociales, peut avoir un effet ambivalent sur la susceptibilité au phishing. Les extravertis peuvent être plus exposés aux tentatives de phishing par des canaux comme les réseaux sociaux, où les escroqueries se présentent souvent sous forme de messages ou de sollicitations provenant d'amis ou de contacts. Leur tendance à établir des liens sociaux rapides peut les amener à accorder une confiance excessive, même à des inconnus, ce qui peut les rendre plus vulnérables [23]. Cependant, l'extraversion peut aussi parfois les rendre plus conscients de la nécessité de sécuriser leurs interactions en ligne, selon le contexte [37]. D'autre part, les individus peu extravertis ne divulguaient pas leurs mots de passe et étaient perçus comme insociables [14].

Les personnes qui sont très **agréables**, donc coopératives et enclines à aider les autres, peuvent également être plus vulnérables aux attaques de phishing, car elles sont plus susceptibles de faire confiance à des personnes inconnues ou d'accepter des demandes sociales qui leur sont adressées [23] [25]. Une personne agréable pourrait être moins sceptique et plus susceptible de répondre positivement à des messages soi-disant amicaux ou utiles, comme des demandes d'informations personnelles. L'impulsion d'aider, même à distance, peut amener à cliquer sur un lien malveillant si cela semble bénéfique à quelqu'un dans le besoin.

Enfin, les personnes avec un haut niveau de **névrosisme** (c'est-à-dire une propension à ressentir de l'anxiété, de la nervosité, ou de l'angoisse) sont plus susceptibles de tomber dans des pièges de phishing [26] [27].

Cela peut s'expliquer par plusieurs facteurs :

- Réaction émotionnelle excessive : les personnes très anxieuses peuvent être moins attentives et plus réactives face à des messages qui suscitent des émotions, comme des alertes de sécurité ou des offres urgentes.
- Tendance à la peur de perdre ou à la panique : le phishing exploite souvent des sentiments d'urgence ou de danger. Une personne nerveuse pourrait réagir rapidement sans vérifier, augmentant ainsi le risque de tomber dans un piège.

5 – FRAUDE AU PRÉSIDENT – QUELS SONT LES TRAITS DE PERSONNALITÉS LES PLUS FAVORABLES.

Il n'existe pas de littérature connue à ce jour qui explore ces traits de personnalité dans un contexte spécifique de fraude au Président. Toutefois, on peut extrapoler les résultats obtenus dans les études précitées et en tirer des intuitions qu'il faudrait valider en mettant en place des études appropriées.

L'ouverture à l'expérience
Les personnes ayant un score élevé en ouverture à l'expérience sont souvent curieuses et analytiques. Dans un contexte de fraude au Président, elles pourraient être plus aptes à remettre en question une demande inhabituelle ou à chercher des informations complémentaires avant de se conformer. À l'inverse, celles qui affichent une faible ouverture risquent de suivre des directives de manière plus automatique, sans s'interroger sur la validité du message, renforçant ainsi le biais d'autorité.

La conscienciosité
Les personnes très consciencieuses sont généralement rigoureuses, organisées et attentives aux détails. En théorie, elles pourraient être moins enclines à suivre aveuglément une demande inhabituelle, notamment si elles ont l'habitude de vérifier la légitimité des requêtes sensibles. Toutefois, dans le cadre d'une attaque de fraude au Président où l'urgence est souvent accentuée, même ces individus peuvent être poussés à agir rapidement, surtout si la demande semble provenir d'un cadre supérieur auquel ils sont habitués à faire confiance.

L'extraversion
L'extraversion, associée à la sociabilité et à la recherche d'interactions, ne présente pas un lien direct évident avec la vulnérabilité au biais d'autorité. Cependant, les extravertis, en raison de leur orientation vers les relations interpersonnelles, pourraient être plus enclins à accorder leur confiance aux messages provenant d'un individu en phase avec leur environnement professionnel.

L'agréabilité
Les personnes avec un score élevé en agréabilité sont souvent caractérisées par leur confiance et leur propension à coopérer. Dans un contexte de fraude au Président, ces individus peuvent être particulièrement vulnérables à l'autorité usurpée, car ils ont tendance à croire et à se conformer aux instructions venant de figures perçues comme légitimes. La sollicitation d'un supérieur hiérarchique fictif peut ainsi déclencher une réponse automatique et peu critique.

Le neuroticisme
Un niveau élevé de neuroticisme se traduit souvent par une sensibilité accrue au stress et à l'anxiété. Face à un message alarmant qui exploite le biais d'autorité et une situation d'urgence, ces personnes peuvent se laisser submerger par l'émotion, ce qui réduit leur capacité à analyser rationnellement la demande. L'anxiété provoquée par une potentielle crise ou une menace pour l'entreprise peut ainsi favoriser une réaction impulsive.

Dans le contexte d'une fraude au Président, les cybercriminels combinent plusieurs leviers : l'urgence, la personnalisation du message et l'usurpation d'une autorité. Cette stratégie pourrait profiter particulièrement à des individus ayant des traits de personnalité spécifiques, tels que :

- Une **agréabilité élevée**, qui encourage la confiance et la conformité,
- Un **neuroticisme élevé**, qui accroît la réactivité émotionnelle face aux situations stressantes,
- Une **faible ouverture à l'expérience**, qui limite la tendance à remettre en question une directive provenant d'une figure d'autorité.

On pourrait donc imaginer que ces personnes se situent dans une zone à risque maximal en cas de fraude au Président. A contrario, des profils avec une ouverture plus importante ou une moindre réactivité émotionnelle pourraient figurer dans une zone moins vulnérable, où la propension à douter ou à vérifier l'authenticité d'une demande est plus élevée.

Ainsi, même si chaque trait agit différemment, l'interaction de ces caractéristiques dans un environnement de travail peut créer une vulnérabilité spécifique face à ce type d'attaques. Il est important de noter que la situation contextuelle (pression temporelle, personnalisation du message, historique relationnel avec les supérieurs) joue également un rôle crucial dans la manière dont ces traits influencent la réaction face à une sollicitation frauduleuse.

Comme nous venons de le constater, les études existantes semblent démontrer une corrélation entre certains traits de personnalité et la susceptibilité au phishing, confirmant ainsi notre première hypothèse (H1). Pour autant, afin de la valider dans un contexte de fraude au Président, il faudrait mener des campagnes de simulation d'attaques auprès des publics concernés, en utilisant les biais et les leviers psychologiques déjà décrits. Il conviendrait ensuite de faire passer le test de personnalité Big 5 aux personnes cibles afin de confirmer/infirmer cette corrélation.

Ainsi, ces résultats pourraient ainsi être utilisés pour développer des outils de dépistage permettant de déterminer quels individus sont les plus vulnérables aux tentatives de spear phishing dans un contexte de fraude au Président, de mettre en place des programmes de formation, de remédier à ces vulnérabilités et de réduire les risques de sécurité.

6 – EXPLOITER LES TRAITS DE PERSONNALITÉS POUR REDUIRE LA RÉPONSE AUX ATTAQUES DE FRAUDE AU PRÉSIDENT

Comme nous venons de le voir, la nécessité d'un cadre de cybersécurité qui intègre des connaissances comportementales est indispensable à une résilience organisationnelle face aux attaques par ingénierie sociale telles que la fraude au Président.

Les entreprises qui utilisent des tests de personnalité tels que le Big 5 pour recruter leurs collaborateurs, pourraient également exploiter les résultats de ces tests pour profiler les personnes présentant un risque cyber, notamment pour des collaborateurs sensibles qui, de par leurs prérogatives, sont susceptibles de procéder à des transferts financiers ou à communiquer des informations de premier plan.

Certes, l'utilisation du résultat de ses tests dans un cadre cyber ne doit pas être déterminante dans la prise de décision pour l'embauche d'un collaborateur, mais peut orienter des actions de sensibilisation et de formation plus ciblées, à mettre en place à posteriori, selon le profil de l'individu.

Pour ce qui est des collaborateurs déjà en fonction, et avec leur accord, le passage du test Big 5 pourrait là aussi permettre de détecter les faiblesses de chacun et de mettre en place les actions adéquates.

En tenant compte des points abordés dans cette étude, on pourrait envisager la mise en place du plan d'action suivant , qui resterait à valider pour en démontrer l'efficacité.

Il conviendrait en premier lieu de faire une campagne de fraude au Président au travers de spear phishing interne à l'entreprise, en direction de collaborateurs ayant un niveau de responsabilité les autorisant à faire des transactions financières (comptabilité, paie, RH), ceci afin de voir le taux d'hameçonnage et d'avoir une valeur étalon. Une fois cette campagne menée, les collaborateurs cibles passent le test Big 5 afin de déterminer leurs traits de caractères individuels.

A la lumière de ces informations, nous réunissons les collaborateurs afin de mener les actions suivantes :

- Une présentation du contexte de la cybercriminalité lié à la fraude au Président, en décrivant les différents aspects psychologiques de ce type d'attaque (biais, situation d'urgence…).

- Identification par chaque individu des faiblesses potentielles révélées par le test Big 5 passé précédemment et des points de vigilance individuels à avoir en fonction des résultats (à rapprocher des leviers psychologiques utilisés par les attaquants).

- Travail sur les biais cognitifs au travers d'un jeu de cartes présentant les biais sous forme ludique [28] avec des mises en situation. Ici, le « learning by doing » confronte le sujet à ses propres biais, dans un cadre sans risque, et lui fait prendre conscience de ses vulnérabilités.

- Travail sur les notions d'autorité, de stress lié aux sentiments d'urgence, de peur, au travers de jeux de rôle ou de discussions collectives, pour voir comment diminuer les déclencheurs émotionnels qui permettent d'avoir une approche plus attentive aux demandes d'informations qui semblent urgentes ou autoritaires.

- Etude d'e-mails de spear phishing en en décortiquant les différents aspects en relation avec les leviers psychologiques évoqués lors d'une fraude au président. Chacun peut ainsi se situer par rapport à ses faiblesses et identifier les points d'accroche des attaquants.

- Enfin, rédiger collectivement un e-mail de spear phishing afin de se mettre dans la peau d'un attaquant (recherche d'informations sur le net pour la personnalisation, rédaction d'un e-mail en utilisant les ressorts psychologiques etc.).

Une fois cette action de sensibilisation effectuée, il faudra, à distance, mener une nouvelle campagne de fraude au Président afin de confirmer/d'infirmer l'hypothèse n°2 de cette étude, qui suggérait que la mise en place d'actions ciblées au sein des services financiers, utilisant les résultats de tests individuels, permettrait d'améliorer la vigilance des collaborateurs de façon significative, en leur faisant prendre conscience de leurs fragilités intrinsèques.

7. CONCLUSION ET PERSPECTIVES

Cet article a examiné les aspects psychologiques qui contribuent à la sensibilité des individus aux attaques de fraude au Président, en mettant particulièrement le focus sur les différents aspects de la personnalité. On a pu voir que certains profils personnels sont plus propices à y répondre favorablement.

Dans ce contexte, l'exploitation des résultats du test Big 5 pourrait permettre d'identifier les faiblesses des collaborateurs et de mettre en place des actions de sensibilisation ciblées, en travaillant sur l'ensemble des leviers psychologiques utilisés par les hackers, et en les objectivant par rapport aux traits de personnalité des individus, dans un contexte de fraude au Président.

Dans cette optique, pour confirmer/infirmer la réduction de la réponse aux attaques des populations susceptibles d'engager des transactions financières, tel que nous l'avons évoqué dans cette étude, il faudrait mener une action de sensibilisation comme décrite précédemment et en mesurer les effets à court et moyen terme.

Dans tous les cas, une approche uniquement techno-centrée de la cybersécurité, nous le savons maintenant, n'est plus pertinente. Seule une démarche basée à la fois sur les sciences dures et les sciences humaines pourra apporter des éléments de réponse pour enrayer ce phénomène.

Références

[1] Direction de l'information légale et administrative (2024). Le bilan 2023 des cyberattaques contre les entreprises https://entreprendre.service-public.fr/actualites/A17303

[2] Fraudologie (2021). Psychologie de la fraude au Président https://open.spotify.com/episode/52c1KMNxzCdJiZzJzeg5Gu

[3] Cho, J.-H., Cam, H. Oltramari, A. (2016). Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis. *International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, 7-13, 10.1109/COGSIMA.2016.7497779

[4] Teboul, B. (2022). Le tournant cognitif de la cybersécurité : changement de paradigme et prolégomènes à la cybersécurité cognitive. https://hal.science/hal-03639141/document

[5] Avey, C. (2023), " The Impact of AI on Social Engineering Cyber Attacks https://www.secureworld.io/industry-news/impact-ai-social-engineering-attacks.

[6] Verizon (2024). 2024, Data breach investigation report https://www.verizon.com/business/en-gb/resources/reports/2024/dbir/2024-dbir-data-breach-investigations-report.pdf

[7] CNIL (2021). Violation du trimestre : le faux ordre de virement international ou « fraude au président » https://www.cnil.fr/fr/violation-du-trimestre-le-faux-ordre-de-virement-international-ou-fraude-au-president

[8] Découvrir l'univers des biais cognitifs, https://biais-cognitif.com/

[9] Tversky, A, Kahneman,D. (1974). Judgment under Uncertainty: Heuristics and Biases: Biases in judgments reveal some heuristics of thinking under uncertainty. *Science* Vol 185, Issue 4157, 1124-1131, 10.1126/science.185.4157.112

[10] Milgram, S. (1965). Some Conditions of Obedience and Disobedience to Authority. *Human Relations*, 18(1), 57-76. https://doi.org/10.1177/001872676501800105

[11] Ni, F., Arnott, D., Gao, S. (2019). The anchoring effect in business intelligence supported decision-making. *Journal of Decision Systems*, vol. 28, 67–81, 10.1080/12460125.2019.1620573

[12] The décision lab (2023). Simple effet d'exposition. Pourquoi préférons-nous les choses qui nous sont familières ? https://thedecisionlab.com/fr/biases/mere-exposure-effect

[13] Kavvadias, Alexandros & Kotsilieris, Theodore. (2025). Understanding the Role of Demographic and Psychological Factors in Users' Susceptibility to Phishing Emails: A Review. *Applied Sciences*. 15. 2236. 10.3390/app15042236.

[14] Rahman, A., Al-Obeidat, F., Tubaishat, A., Shah, B., Anwar, S., Halim, Z. (2022). Discovering the correlation between phishing susceptibility causing data biases and big five personality traits using C-GAN. *Transactions on Computational Social Systems*, 1-9, 10.1109/TCSS.2022.3201153

[15] Bright, C. Wziatka, M., Ngaruko, W. (2022). An examination of the role of big five personality traits, cognitive processes and heuristics on individuals' phishing attack susceptibility levels. 10.31234/osf.io

[16] Eftimie, S., Moinescu, R., Răcuciu, C. (2022). Spear-phishing susceptibility stemming from personality traits. 10.1109/ACCESS.2022.3190009

[17] Costa, P.T., McCrae, R. (1992). Four ways five factors are basic. *Personality and Individual Differences, vol 13*, 653-665, 10.1016/0191-8869(92)90236-I

[18] Plaisant O., Courtois R., Réveillére C. et al. () Validtion par analyse factorielle Du Big Five Inventory français (BFI-fr). Analyse convergente avec le NEI-PI-R, Ann Med Psychol, 97-106

[19] Goldberg LR. An alternative “description of personality”: The big-five factor structure. J Pers Soc Psychol 1990;59:1216-29.

[20] Goldberg LR , The developpement of makers for the big-five factor structure, Psycchil Assess 1992 4 26-42

[21] McCrae, R. R. & Costa, P. T. (1990). Personality in adulthood. *New York: The Guildford Press.*

[22] Vishwanath, A., Herath, T., Chen, R., Wang, J., Rao Raghav, H. (2011). Why do people get phished ? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, vol 51,* 576-586, 10.1016/j.dss.2011.03.002

[23] Alseadoon, I., Othman, M., Fairuz, I., Chan, T. (2015). What Is the Influence of Users’ Characteristics on Their Ability to Detect Phishing Emails ? *Electrical Engineering, vol 315*, 949-962, 0.1007/978-3-319-07674-4_89

[24] Halevi, T., Lewis , J., Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. *Proceedings of the 22nd International Conference on World Wide Web,* 10.1145/2487788.2488034

[25] Pattinson, M., Parsons, K., Jerrram, C., McCormac, A. (2012). Why do some people manage phishing e-mails better than others ? *Information Management & Computer Security, vol 20,* 18-28, 10.1108/09685221211219173

[26] Vishwanath, A. (2015). Examining the distinct antecedents of e-Mail habits and its influence on the outcomes of a phishing attack. *Journal of Computer-Mediated Communication,* Volume 20*,* 570-584, 10.1111/jcc4.12126

[27] Jansson, K. (2011). A model for cultivating resistance to social engineering attacks. *Ph.D. Thesis, Nelson Mandela Metropolitan University*, 10.3390/fi11030073

[28] Medium (2023). Un serious game open source sur les biais cognitifs !
https://medium.com/maif-data-design-tech-etc/un-serious-game-open-source-sur-les-biais-cognitifs-7a5e27164577