PRODEVAL

INGÉNIERIE DES SOLUTIONS GAZ

Analyse de la campagne de prévention "Phishing" (23/01/2024 à 05/02/2024)
DSI

Introduction au "Phishing"

- Le "Phishing" est une tactique de cybercriminalité où des individus malveillants utilisent des e-mails, des messages instantanés ou des appels téléphoniques pour tromper les utilisateurs et les inciter à divulguer des informations sensibles telles que des identifiants de connexion, des numéros de carte de crédit ou d'autres données personnelles.

- Les attaquants utilisent souvent des techniques de manipulation psychologique et usurpent l'identité de sites Web pour inciter les victimes à partager des données en toute confiance.

Introduction à la simulation de "Phishing"

- Une simulation de "Phishing" consiste à mettre en oeuvre de fausses attaques. Elles entrent souvent dans le cadre d'une stratégie globale de sensibilisation des employés à la cybersécurité.

- Les entreprises utilisent des outils spécialisés pour envoyer de faux e-mails de "Phishing" à leurs employés, reproduisant les tactiques utilisées par les cybercriminels. L'objectif est de sensibilier les utilisateurs à la reconnaissance d'indices qui doivent attirer leur attention et les rendre plus vigilants.

Objectifs de la campagne de prévention "Phishing"

Prise de conscience

- Identifier les indices d'une tentative de "Phishing" dans un email.
- Comprendre les conséquences de la divulgation d'informations sensibles.
- Reconnaître les pratiques et les tactiques de manipulation des cybercriminels.

Évaluation des risques

- Identifier les vulnérabilités spécifiques de l'organisation face au "Phishing".
- Déterminer les secteurs ou équipes les plus à risque.
- Évaluer l'impact financier ainsi que sur la réputation de

Formation Continue

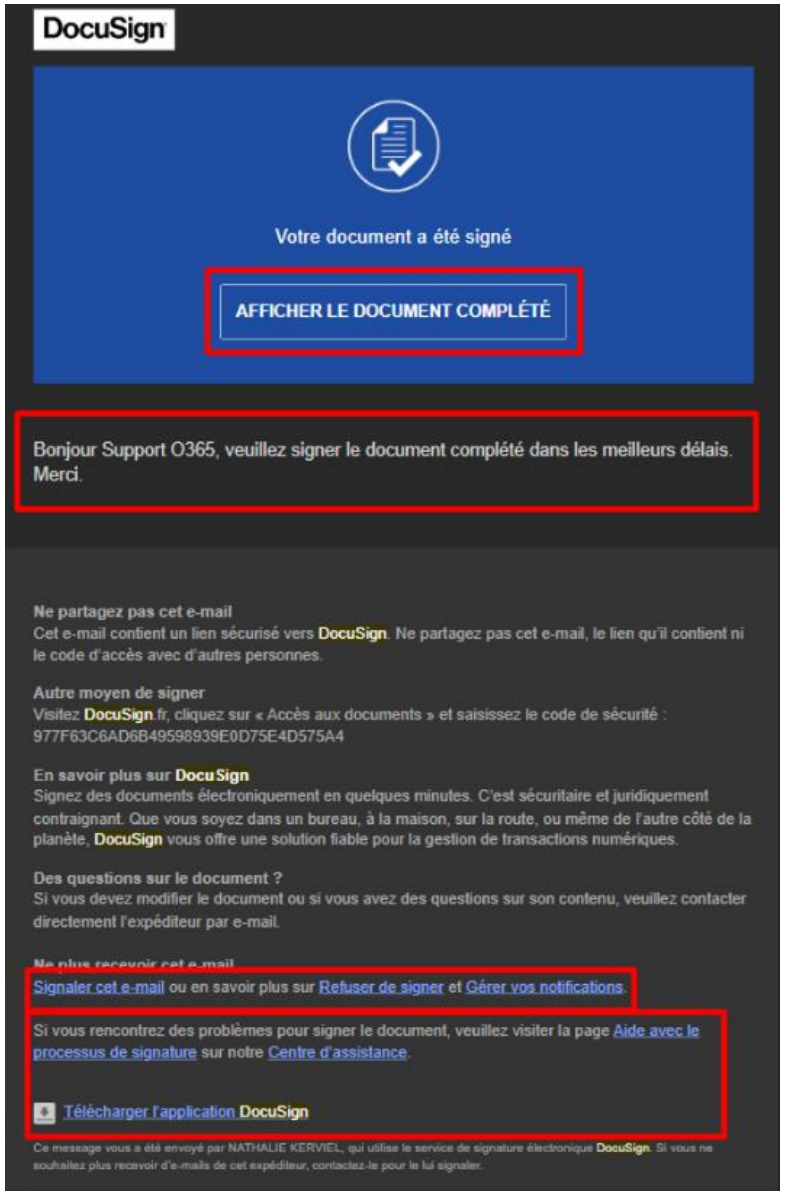
- Dispenser des formations régulières sur la prévention du "Phishing".
- Informer sur les dernières techniques de "Phishing".
- Réaliser des simulations fréquentes pour tester la réactivité des utilisateurs.

Scénario de la campagne

Le service informatique a déployé une simulation de "phishing" en envoyant un e-mail suspect aux utilisateurs de l'entreprise. L'objectif était de les sensibiliser et d'attirer leur attention sur la nécessité d'être vigilant au quotidien.

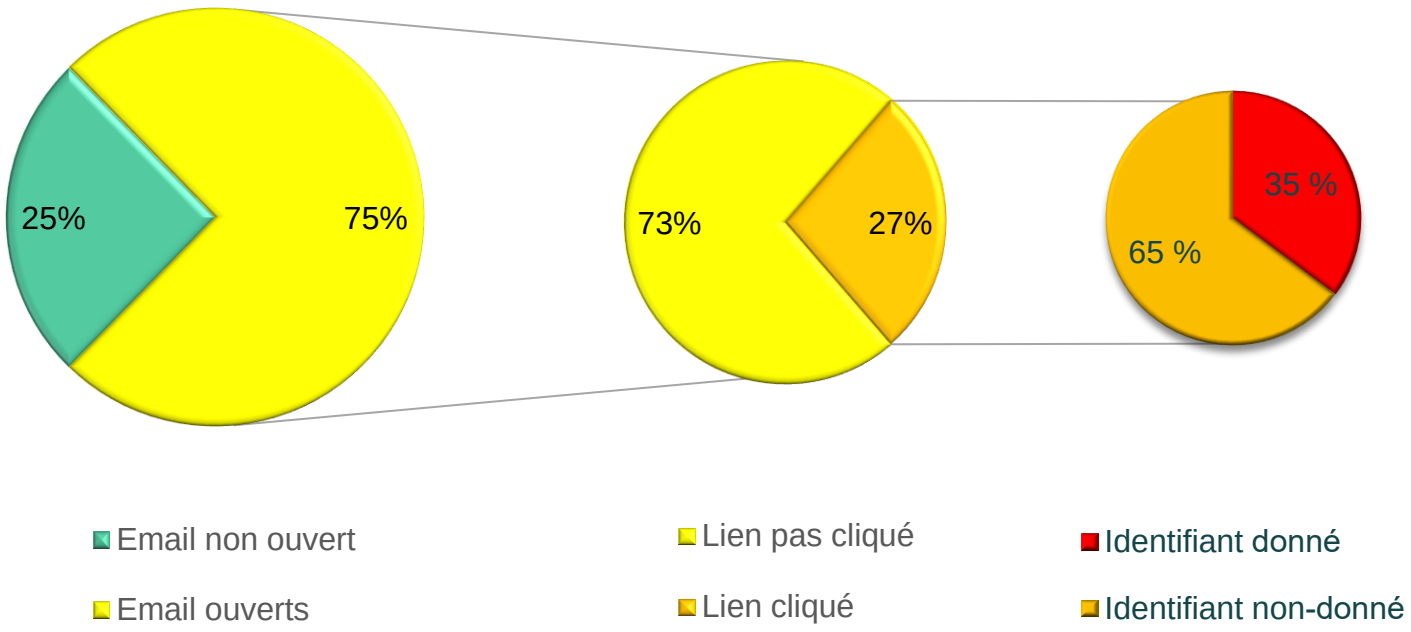
Dans notre simulation, nous avons opté pour un e-mail provenant de DocuSign, auquel nous avons apporté quelques modifications.

- **Le nom de domaine :** Les pirates utilisent souvent des noms de domaine connus en les changeant légérement afin de créer un sentiment de confiance et de tromper les utilisateurs.
- **Les liens du mail :** Les liens contenus dans l'email, liens qui doivent normalement rediriger vers le site de DocuSign, ont été remplacés par des liens suspects. Ceci est facilement vérifiable en passant la souris sur ces liens. Les pirates utilisent en effet souvent des noms de sites web ressemblants à des sites de confiance afin de tromper les utilisateurs.
- **Le texte du mail :** Le texte est rédigé dans un style professionnel dont l'objectif est de tromper la vigilance de l'utilisateur.



Analyse

Résultats



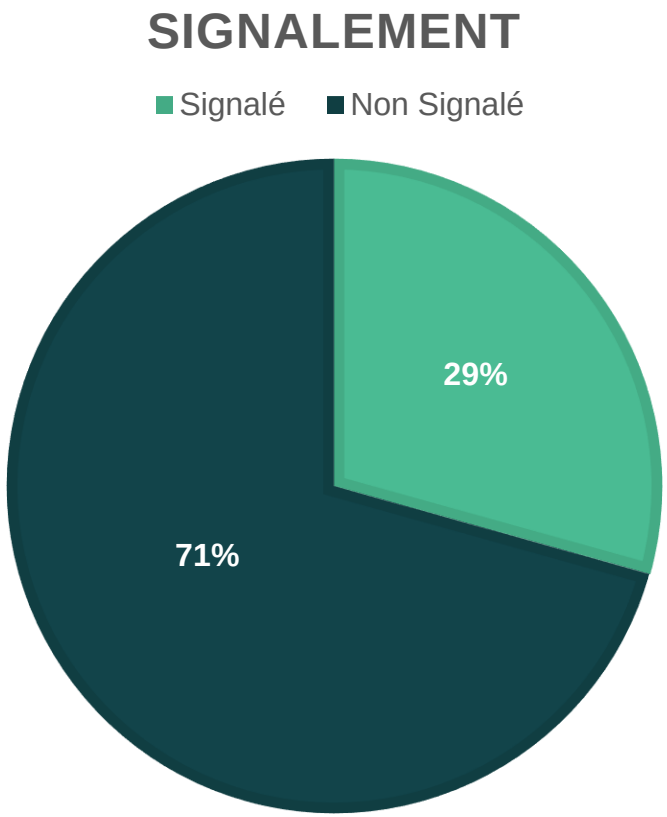
- Parmi les 433 utilisateurs ciblés par la campagne de "Phishing", 25% n'ont pas ouvert le mail. Notons que l'ouverture d'un mail à ce stade n'est pas considérée comme une erreur.
- 75% ont ouvert le mail.
- Sur ces 75%, 73% n'ont pas cliqué sur le lien, tandis que 27% ont commis une première erreur : cliquer sur le lien. Il était en effet possible de constater que l'adresse vers laquelle conduit le lien était suspecte en passant la souris dessus.
- Parmi les 27% qui ont cliqué, 57% n'ont pas fourni d'identifiant de connexion, mais 35% l'ont fait, ce qui constitue une faille de sécurité majeure.
- **En conclusion, 7% des utilisateurs ciblés (soit 31 personnes au total) ont été piégés et auraient potentiellement mis en danger les données de l'entreprise dans le cas d'une vraie tentative de "Phishing".**

Usage de l'option "Signaler" dans Outlook

Signaler un email suspect est essentiel car cela permet de déclencher des mesures de sécurité et de contrer les menaces potentielles.

En signalant un e-mail suspect, les utilisateurs contribuent à se protéger et à protéger l'entreprise

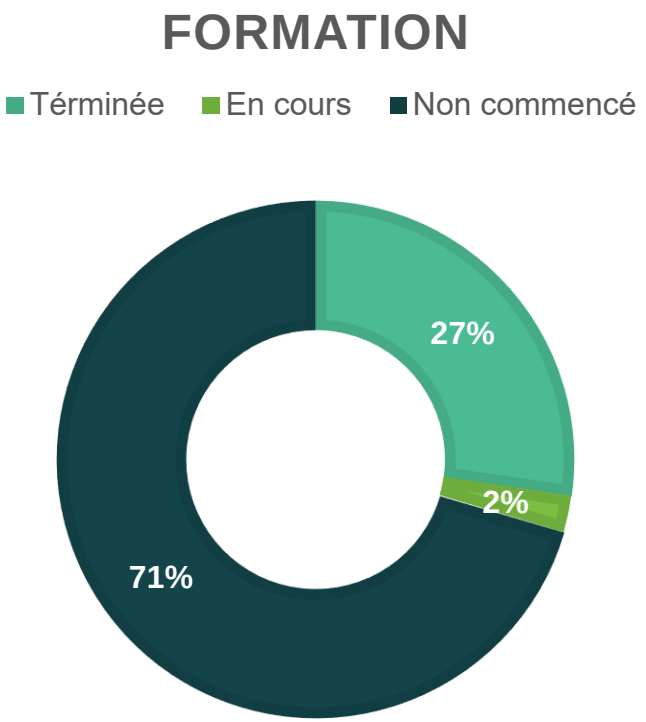
Nous constatons que **71 %** des utilisateurs n'ont pas signalé l'email suspect



Formation de prévention

Les formations de prévention proposées proposent un questionnaire comprenant des choix multiples ou des questions vrai/faux pour évaluer les connaissances des utilisateurs sur le "Phishing". Ces questionnaires visent à fournir des explications détaillées sur:

- Les techniques utilisées dans les attaques de phishing.
- Les indices à reconnaître pour se protéger d'une tentative de "Phishing".
- Les meilleures pratiques pour éviter les escroqueries en ligne et protéger ses informations personnelles.



Le graphique illustre la répartition des utilisateurs ayant commis une erreur en cliquant sur un lien d'e-mail frauduleux et ayant été assignés à une formation de sensibilisation au phishing. Parmi eux, **71%** n'ont pas encore commencé la formation, **27%** l'ont terminée, et **2%** sont en train de l'effectuer. À noter que ceux qui ont fourni leurs identifiants de connexion après avoir cliqué sur le lien reçoivent deux formations.

Axes d'amélioration

Suite à la campagne de prévention au "Phishing" menée, plusieurs conclusions peuvent être tirées :

1. **Niveau de sensibilisation :** Les résultats montrent que malgré une sensibilisation préalable, un pourcentage significatif d'employés est tombé dans le pièges. Cela souligne le besoin d'une sensibilisation continue et approfondie pour renforcer la vigilance de l'ensemble du personnel face à de telles menaces.2.
2. **Manque de vigilance malgré la présenced' indices :** Le pourcentage élevé d'employés ayant ouvert les e-mails et même cliqué sur les liens montre qu'il y a des lacunes dans la reconnaissance des signaux d'alerte du "Phishing". Des efforts supplémentaires sont nécessaires pour sensibiliser les employés à ces indices et les inciter à adopter des comportements plus prudents en ligne.
3. **Nécessité de répéter ces exercices de simulation et de la formation:** Les résultats soulignent l'importance des simulations de "Phishing" et des formations régulières. Ces exercices permettent de maintenir la vigilance des employés, de les familiariser avec les dernières tactiques des cybercriminels et de renforcer leurs compétences en matière de détection et de gestion des attaques de "Phishing".
4. **Promotion de l'usage de l'option "Signaler" dans Outlook :** Les employés doivent être encouragés à signaler tout e-mail suspect dès sa réception afin de permettre une intervention rapide et efficace de la part des équipes de sécurité.

PRODEVAL

INGÉNIERIE DES SOLUTIONS GAZ

www.prodeval.com