Filière Informatique de gestion
Studiengang Wirtschaftsinformatik

Hes·so VALAIS WALLIS

Évaluation du *Social Engineering* en environnement académique

Étudiante : Montaine Burger
Professeure : Natalie Sarrasin

Résumé

1. Analyse et tests d'utilisation d'outils de *Security Awareness* pour la HES-SO Valais-Wallis
2. Évaluation du niveau de sensibilisation — *Social Engineering* — actuel d'un échantillon cible
3. Recommandations de formations / sensibilisation à mettre en place

Introduction

- Aucune entreprise n'est à l'abri de subir une attaque informatique pouvant être **lourde de conséquences** : vol de données, pertes financières et surtout détérioration de la réputation.
- La société peut posséder les technologies les plus à jour en matière de sécurité et avoir entraîné ses employés comme des experts ; elle n'en sera pas moins **totalement vulnérable**. Les individus peuvent avoir suivi les meilleures pratiques de cybersécurité, installé tous les outils recommandés et être vigilants dans toutes leurs tâches ; ils seront toujours ébranlables et imparfaits.
- Car le véritable maillon faible de la cybersécurité, c'est **le facteur humain**.

Déroulement du travail

- **Planification du projet** avec l'entreprise mandante : établissement des étapes-clés et définition des besoins
- Découverte du **contexte du *Social Engineering*** : description des formes d'attaque et du *modus operandi*
- Définition des **cibles du *Social Engineering*** : recherche de profils génériques et adaptation au niveau académique
- Analyse des **outils de *Security Awareness*** : évaluations fonctionnelle et technique, et conception d'une matrice de classification
- Mise en place d'une **simulation d'attaque** : élaboration des scénarios et lancement des campagnes de *phishing*
- **Évaluation des résultats** des campagnes : désamorçage de l'échantillon ciblé et récolte des *feed-backs*
- **Recommandations et prescriptions** : bonnes pratiques liées à la sécurité de l'information et recommandations de sensibilisation à mettre en place

Outils analysés

Lucy

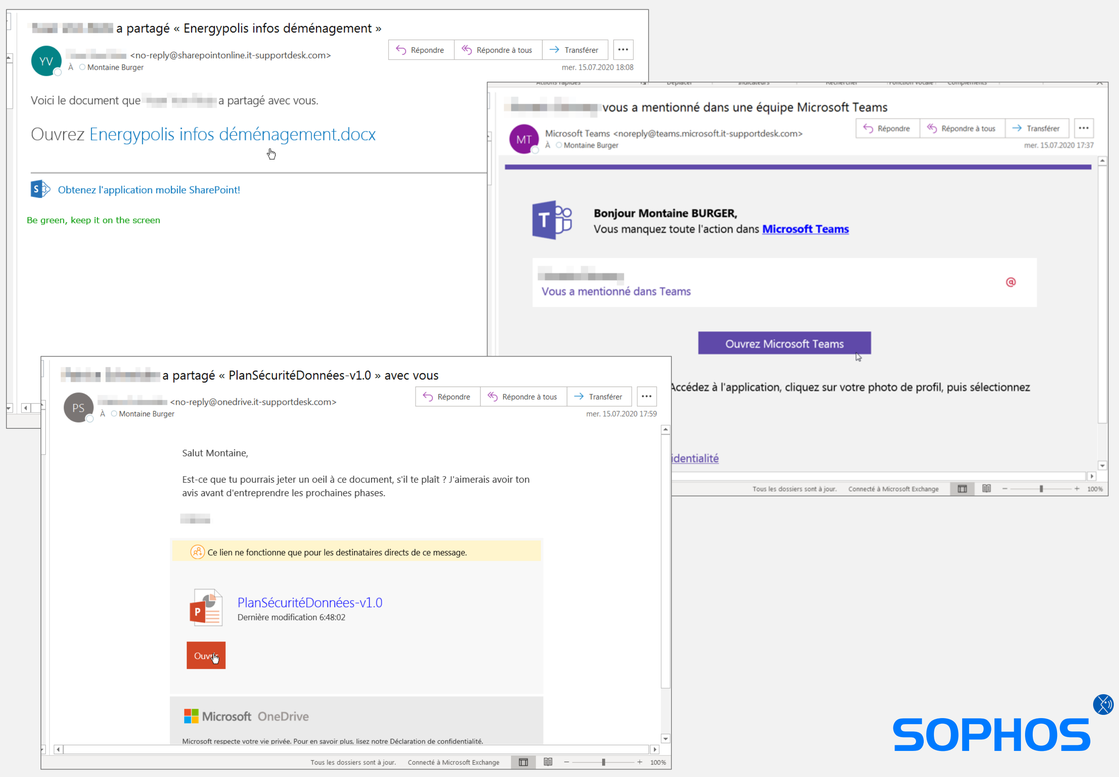
proofpoint

SOPHOS

WEBROOT

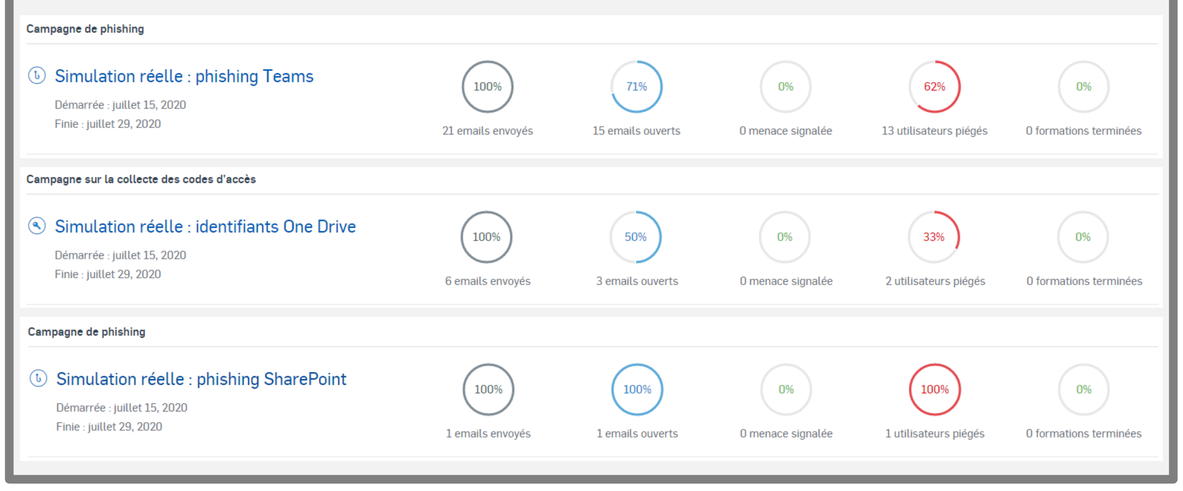
SoSafe
Cyber Security Awareness

Modèles de simulation de *phishing*



SOPHOS

Résultats observés



Conclusions

- La **qualité des copies** frauduleuses — de pages internet ou de standards d'e-mails — augmente de manière considérable ; l'authenticité visuelle des modèles était telle que bon nombre des cibles se sont fait duper.
- Il était **relativement aisé de configurer un outil de *Security Awareness*** pour une utilisation en environnement académique.

Contact et informations supplémentaires :
http://www.hevs.ch/ig

Valais excellence CERTIFIED