Réalisation des campagnes de phishing

Nadège GRANDYOT

Projets en entreprise

Contexte

La sensibilisation à la cybersécurité doit permettre à un collaborateur de comprendre les risques constants et a appliquer les bons reflexes cyber en parallèle de ses fonctions. Un enjeu de taille chez Engie Home Services où plus de la moitié des salariés sont des cols bleus qui se servent peu de leurs équipements informatiques. Il à été mis en place un système de test de phishing en interne pour familiariser les collaborateurs avec ces méthodes d’arnaques.

L’outils et organisation d’une campagne

L’outil utilisé est KnowBe4, logiciel permettant d’organiser ce genre de campagne de test et est dédié à la formation a la sécurité informatique. Une fois la date de la campagne et les destinataires choisies (en fonction des directions pour adapter le contenu de la campagne), il faut créer le Template de phishing. Il faut qu’il ressemble au plus à un mail de phishing ; contenu trop avantageux pour être vrai, fautes d’orthographes, lien douteux… Puis envoi du mail par la plateforme KnowBe4. Si l’utilisateur clique sur le lien et entre ses informations de connexion, il arrive sur une page indiquant qu’il s’est fait avoir. Voici un exemple :

⚠ Chèques vacances restants

C CSEngie <ces.engie@engiehomeservices.fra>
À GRANDYOT Nadege (ENGIE Home Services)

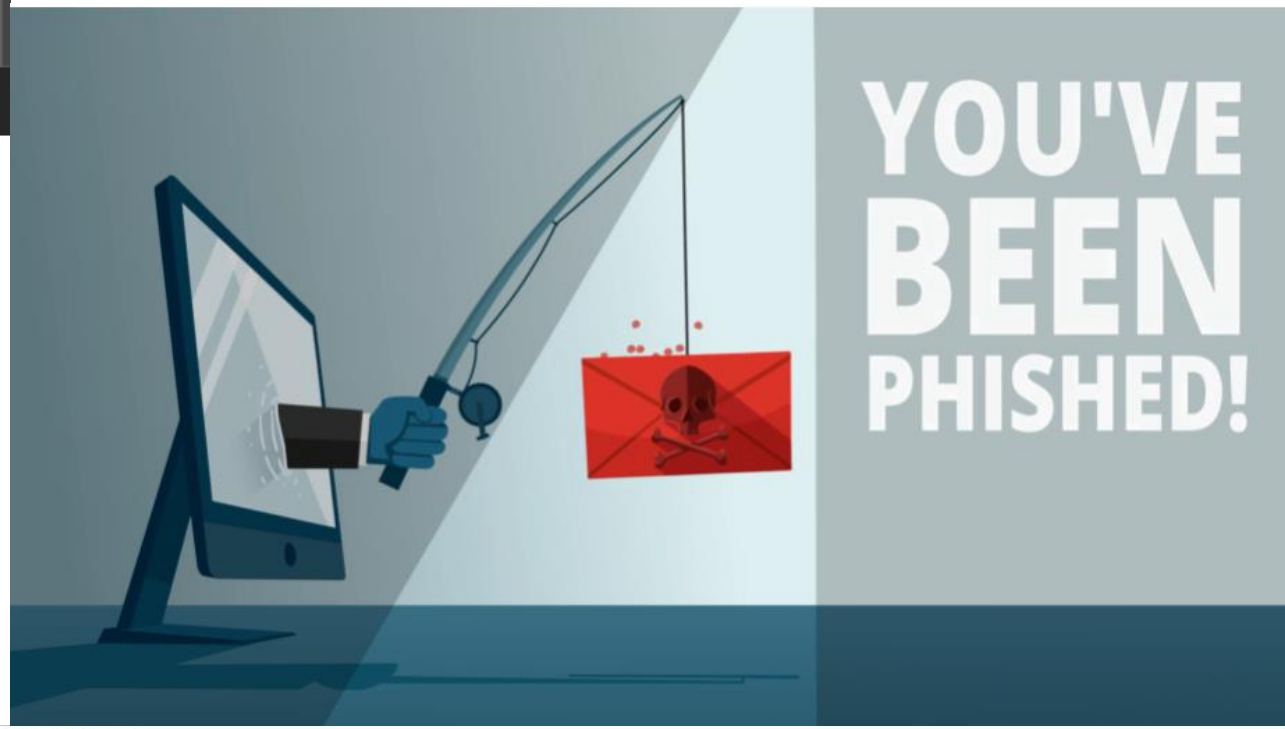
Bonjour,

Suite à la distribution de chèques vacances, nous avons beaucoups de carnets restants.
Nous les distiburons aux personnes qui en font la demande.
Pour cela, cliquez sur ce lien puis authentifiez vous:
Lien page CSE/carnetchequesvacances.engie.fra
Depéchez-vous, il n'y en aura pas pour tout le monde...

Cordialement,
Votre CSE

Exemple de mail

Message si l'utilisateur clique sur le lien et s'authentifie ←



*vous avez été hameçonné

CECI N'EST QU'UN TEST.

Il s'agissait d'un test d'hameçonnage simulé qui vous a été envoyé par votre organisation. Vos fichiers n'ont PAS été chiffrés et ne seront PAS détruits. Mais s'il s'agissait d'une véritable attaque, les cybercriminels auraient pu voler vos informations sensibles, puis les corrompre, les détruire, les retenir contre rançon ou même les vendre en ligne.

N'oubliez pas ces trois règles pour rester en sécurité en ligne :

01
Arrêtez-vous toujours, regardez et réfléchissez avant de cliquer! Verifiez l'expéditeur, l'orthographe, la police, la cohérence, les logos...

02
Vérifiez les e-mails suspects auprès de l'expéditeur via un autre support (exemple: telephone, teams, en face...).N'hésitez pas à demander conseil à votre supérieur ou collègue/s.

03
En cas de doute utilisez le bouton:
Phish Alert Report
Phish Alert

Veuillez suivre la formation en ligne en cliquant sur ce lien : U.Learn

KnowBe4 Veuillez noter : ce message provient de KnowBe4, Inc. et non de la société dont le nom est mentionné dans le corps du message électronique, car la société n'a aucune association avec KnowBe4, Inc. et n'approuve pas les services de KnowBe4, Inc. Le but de ce message est de démontrer comment les attaques de phishing peuvent provenir d'e-mails qui semblent provenir de sociétés réputées.

Exemple de calendrier prévisionnel de campagnes de phishing

DATE	Colonne2	QUI?	Echecs
15-janv	retour de vacances		
01-mars		Techniciens	280 (10%)
11-avr	vacances scolaires		
15-avr	fin de la periode de chauffe		742 (13,2%)
25-mai	Inventaire véhicules ⚠ 31 mai-> maintenance	Direction des achats	
16-juin	Inventaire magasins	Direction des achats	3 (21,4%)
31-juil	Departs en vacances		
30-août	retour de vacances		
01-sept	Rentrée scolaire		
30-oct	Debut periode de chauffe	techniciens?	
15-déc	cloture annuelle	direction financière + dr	