

1. Les attaques MITM : HTTPS
2. Le phishing : Eduquer les visiteurs
3. Les attaques CSRF : Token CSRF
4. Les modifications du DOM : Faire les vérifications au backend
5. Les injections : Figer la forme de la requete SQL et désactiver les balises HTML
6. Le brute force : Mettre une limite sur le nombre d'essais

Pouvez-vous me rappeler ce
qu'est le phishing ?



A votre avis, comment peut-on sensibiliser les visiteurs au phishing ?



1. Actions à mener **avant** une campagne de sensibilisation au phishing
2. Actions à mener **après** une campagne de sensibilisation au phishing
3. **Erreurs à éviter** dans l'élaboration d'une campagne de sensibilisation au phishing

Il faut savoir que mener une campagne de sensibilisation est **plutôt menée pour les collaborateurs** d'une même entreprise que pour les visiteurs externes.

Cela dit, **ces recommandations s'appliquent partout !**

1. Actions à mener **avant** une campagne de sensibilisation au phishing
2. Actions à mener **après** une campagne de sensibilisation au phishing
3. **Erreurs à éviter** dans l'élaboration d'une campagne de sensibilisation au phishing

Actions à mener avant une campagne de sensibilisation

A votre avis, à quoi doit-on
réfléchir avant une campagne
de sensibilisation au phishing ?



1. Construire un **plan de sensibilisation**
avant de planifier une campagne de
phishing

La campagne de phishing est un vecteur de contrôle ainsi qu'un **vecteur d'apprentissage**.

Ainsi, il faut s'assurer que la campagne sera **précédée et suivie d'autres actions** qui permettront aux collaborateurs et aux visiteurs du site d'appréhender le risque phishing, de savoir comment le détecter et comment y réagir

2. Prévenir les collaborateurs et les visiteurs de votre site

D'instinct, les entreprises ont tendance à ne pas communiquer sur la réalisation d'une campagne de phishing, de peur de **fausser les résultats : c'est une erreur !**

Ne pas communiquer en amont, c'est prendre le risque de **frustrer les collaborateurs/visiteurs** et de faire naître de la **résistance vis-à-vis de la cybersécurité.**

Il est important d'être transparent sur l'existence des tests comme sur les raisons de ces tests : **aider les collaborateurs/visiteurs à progresser** et à participer à la défense contre le phishing.

L'objectif étant d'obtenir un état d'esprit **d'union collective contre le risque phishing** et non une opposition des collaborateurs/visiteurs contre votre équipe en terme de sécurité.

De plus, les prévenir peut également permettre
d'augmenter leur vigilance au quotidien.

3. Choisir un scénario adapté

Ne pas viser trop haut : en tant que professionnels, nous sommes généralement mieux formés à la détection du phishing, ce qui nous mène souvent à créer des emails de phishing trop aboutis.

Il est préférable de commencer avec des emails simples et de **monter peu à peu en complexité**. Un email trop complexe pourrait également décourager les collaborateurs et les visiteurs.

Ne pas diviser la campagne : Il n'est pas forcément nécessaire d'envoyer des mails différents à des groupes ciblés car cela dilue les statistiques.

Actions à mener après une campagne de sensibilisation

A votre avis, quelles sont les actions à mener après une campagne de sensibilisation ?



1. Ne pas sanctionner ou dévoiler les collaborateurs ayant été « phishés »

Quelles sont les risques à dévoiler ceux/celles qui se sont fait phishé(e)s ?



Il serait **contreproductif de sanctionner des collaborateurs** ayant été « phishés », et d'autant plus de communiquer leurs noms en interne.

Au-delà de la mauvaise ambiance que ce genre de pratique instaure, le risque serait qu'à l'avenir, **les collaborateurs aient peur d'alerter en cas de doute sur un email**, ou en cas d'incident de sécurité, par peur d'être sanctionnés.

Même une sanction relativement « saine » comme l'obligation de suivre une formation en cas d'erreur lors d'une simulation n'est pas recommandée : les collaborateurs verraient la formation **comme une punition** et elle ne serait pas forcément efficace.

2. Communiquer les résultats

Quel est l'intérêt de
communiquer les résultats ?



En les rendant anonyme, il est primordial de communiquer sur les résultats. Une communication alarmiste desservirait le propos : le marketing de la peur ne fonctionne pas.

La communication doit inclure **une explication sur les moyens de détection du phishing**, ou un lien de redirection vers un espace dédié.

3. Ne pas se focaliser sur les statistiques,
mais sur la montée en compétence des
collaborateurs

L'un des avantages de la campagne de phishing (et c'est ce qui fait sa popularité), c'est qu'elle permet d'obtenir des **résultats mesurables**.

Cependant, il ne faut pas tomber dans le piège des chiffres et se focaliser sur le nombre d'utilisateurs « phishés »

Les conditions de la simulation peuvent **difficilement être identiques** à chaque campagne (l'objet de l'email change, il pourrait être moins attirant pour les collaborateurs, la période de l'année peut être plus ou moins propice, etc.). Il n'est donc **pas forcément adapté de comparer une campagne à une autre.**

L'objectif étant de faire monter en compétences les utilisateurs, il est conseillé de **complexifier petit à petit les emails**. Avoir un ratio d'utilisateurs « phishés » constant **n'est pas problématique** si la complexité des e-mails est différente. Il serait simple d'obtenir des statistiques positives en diminuant la complexité de l'email, et pour autant, le risque serait d'autant plus présent.

L'un des indicateurs qu'il est particulièrement important de regarder est le **taux d'alerte**.

C'est ce que nous attendons des utilisateurs : qu'ils alertent en cas d'email suspect.

4. Former les collaborateurs de manière continue !

Une fois la campagne terminée, et les résultats diffusés, **il faut continuer de sensibiliser les utilisateurs aux risques phishing**. Pour s'assurer que les actions de sensibilisation mises en place sont appréciées et acquises par les collaborateurs, il faut consolider des **indicateurs** d'adhésion.

D'ailleurs, pour que les messages transmis soient plus impactants, nous conseillons toujours de faire des **parallèles entre la vie personnelle et professionnelle**.

C'est d'autant plus vrai à propos du phishing qui cible aussi bien les professionnels que les particuliers. **Une fois que les résultats de la simulation s'améliorent, le niveau de complexité peut être augmenté.**

Erreurs à éviter dans l'élaboration d'une campagne

A votre avis, quels sont les pièges lors de l'élaboration d'une campagne de sensibilisation ?



1. Réaliser des campagnes de sensibilisation
trop complexes

Quel est le risque à réaliser des campagnes trop complexes ?



Réaliser une campagne de phishing doit rester relativement simple. Ne pas trop complexifier la campagne permet des **statistiques uniformes** sur l'ensemble des utilisateurs.

Cela permet également de mettre en place des campagnes de phishing **plus fréquemment**.

2. Ne pas tester continuellement

Quel est le risque à ne pas tester les collaborateurs ou visiteurs souvent ?



Il ne faut pas oublier que la campagne de phishing doit faire partie intégrante d'un plan de sensibilisation, dont l'objectif est de **faire monter les collaborateurs en compétences sur le long terme**, et non juste de pointer leurs lacunes à un instant T.

