Le Phishing ou hameçonnage, qu’est-ce que c’est ?

Utilisant le principe de l'ingénierie sociale, le phishing (ou hameçonnage en français) est une technique frauduleuse destinée à leurrer un internaute pour l’inciter à communiquer des données personnelles en se faisant passer pour un service connu ou un proche. Si les tentatives d’hameçonnage sont aujourd’hui de mieux en mieux réalisées, un mail de phishing présente souvent des signes d’alerte qu’il est possible de déceler : offre alléchante, apparence suspecte, pièce jointe inattendue, adresse d’expédition fantaisiste…

Ces messages ne sont plus toujours dans le français approximatif produit par des traducteurs automatiques ; de plus en plus ils ciblent les utilisateurs grâce à un texte apparaissant plausible. Ils peuvent sembler provenir d’adresses du domaine ens-rennes.fr. Au moindre doute, sur un entête de mail ou sur tout autre informations constituant le mail, demander l'avis au service informatique.

N'ouvrez en aucun cas une pièce jointe dans un mail que vous jugeriez douteux.

Comment repérer un mail de phishing ?

- **Un nom d’expéditeur inhabituel** : La réception d’un message inattendu d’une adresse email inhabituelle, que vous ne connaissez pas ou qui ne fait pas partie de vos contacts, doit éveiller votre attention, même si celle-ci est d’apparence légitime. Si l’adresse email de l’expéditeur vous paraît suspecte, posez-vous les questions suivantes : connaissez-vous l’expéditeur ? Est-il possible que ce dernier vous adresse un message ? Est-ce que le contenu du message vous est réellement destiné ? Est-ce que le sujet abordé vous parle ?

- **Une adresse d’expédition fantaisiste** : La plupart des phishing par email utilisent des adresses de messagerie qui ne ressemblent pas à des adresses officielles. Pour vérifier qu’il s’agit bien d’un message officiel, pensez à vérifier l’adresse email de l’expéditeur. Si cette dernière ne comporte pas le nom de l’entité, qu’elle présente des fautes d’orthographe ou que le nom vous paraît suspect, n’ouvrez pas le message. Il s’agit sûrement d’un mail frauduleux.

- **Un objet d’email trop alléchant ou alarmiste** : L’objet d’un mail de phishing est généralement sommaire et cherche à inciter la victime à ouvrir le message. Un intitulé aguicheur ou inquiétant – comme « remboursement » ou « alerte de sécurité » – qui transmet un sentiment d’urgence inhabituel.

- **Une apparence suspecte** : De nouveaux phishing sont créés chaque jour et les cybercriminels redoublent de créativité pour mettre au point des stratagèmes innovants. Si les méthodes employées sont donc de plus en plus sophistiquées, certains phishing par email revêtent néanmoins une apparence douteuse. Images et logos de mauvaise qualité, flous, déformés,

pixelisés ou pris de loin, peuvent être le signe qu'il s'agit de captures d'écran ou d'éléments volés sur des sites officiels. Idem si le message vous semble légitime mais que son apparence ne semble plus d'actualité (logo désuet). De manière générale, si vous observez des différences entre l'apparence de l'email reçu et celle des mails habituels, méfiez-vous. Il peut arriver que des bugs surviennent mais ces anomalies doivent vous mettre en alerte!

- **Une demande inhabituelle** : Connaître l'adresse email de l'expéditeur n'est pas un critère de confiance absolu : le cybercriminel peut avoir usurpé l'adresse de messagerie d'un proche ou d'un service connu. Remarquez-vous une incohérence, sur la forme ou le fond, entre l'email reçu et ceux que l'expéditeur vous envoie d'habitude ? **Soyez vigilant aux éléments suspects, notamment si le message contient un lien cliquable, une pièce jointe, ou vous demande des informations.**

- **Une incitation à cliquer sur un lien ou une pièce-jointe** : Un mail de phishing cherche généralement à pousser la victime à cliquer sur un lien. Même si le lien semble rediriger vers la page officielle d'un site, il l'amènera sur une page frauduleuse ressemblant beaucoup au site officiel. **Avant de cliquer, pensez à vérifier l'adresse des sites web mentionnés.** Pour cela, positionnez le curseur de votre souris sur le lien proposé sans cliquer afin d'afficher le lien complet et l'adresse où il mène réellement. S'agit-il bien de l'adresse officielle du site annoncé dans le message ? Si l'adresse n'est pas ressemblante, qu'elle est mal orthographiée, qu'elle ne vous dit rien et que le lien vous paraît douteux, il s'agit peut-être d'une tentative d'hameçonnage. **Lisez attentivement les liens avant de cliquer. Parfois, un seul caractère peut changer dans l'adresse du site pour vous tromper.** Pour vérifier que l'adresse correspond exactement à la page de connexion officielle, rendez-vous directement sur le site de l'organisme en question en saisissant manuellement son adresse dans votre navigateur.

Exemples de mails qui doivent vous alerter:

Exemples de mails qui doivent vous alerter:

- Demande de mise à jour ou de confirmation de données personnelles – identifiants, mots de passe, coordonnées bancaires… – par un prétendu organisme public ou commercial de confiance, sous peine de sanction.
- Défaut de paiement ou problème de facturation : un faux mail vous informe qu'un bien ne peut être expédié en raison d'un problème de facturation ou que vous devez régler un impayé.
- Demande de règlement pour éviter la fermeture d'un accès, la perte d'un nom de domaine ou une prétendue mise en conformité RGPD.
- Appel à l'aide : le cybercriminel se fait passer pour un proche, expliquant qu'il se trouve dans une situation désastreuse qui requiert votre aide financière.