La menace croissante du quishing : Comprendre, prévenir et se protéger

Conseils pratiques publié le **26/11/2024**, vu **187 fois**, Auteur : Murielle Cahen

À l'aube du XXIe siècle, l'essor fulgurant des technologies de l'information et de la communication a indéniablement métamorphosé notre mode de vie

Toutefois, cette révolution numérique n'est pas exempte de dangers, et la cybercriminalité s'est développée en parallèle, exploitant les failles inhérentes aux systèmes de sécurité.

Parmi les diverses formes de fraudes en ligne, le quishing — un néologisme résultant de la combinaison des termes « QR code » et « phishing » — représente une menace émergente, préoccupante par son ampleur et sa subtilité. Alors que les codes QR, en raison de leur simplicité d'utilisation et de leur accessibilité, se sont intégrés dans notre quotidien, leur détournement à des fins malveillantes soulève des interrogations cruciales quant à la protection des données personnelles et à la sécurité des transactions électroniques.

Le quishing représente une évolution inquiétante des pratiques de phishing traditionnelles, qui reposaient principalement sur des courriels frauduleux ou des sites web trompeurs.

Le quishing se manifeste principalement par l'insertion de codes QR piégés dans des supports variés, tels que des courriels, des affichages physiques ou des sites internet, incitant les utilisateurs à scanner ces codes dans l'optique de les rediriger vers des sites frauduleux. Ces derniers, souvent conçus pour mimer des plateformes légitimes, peuvent alors subtiliser des informations personnelles, financières ou encore infecter les appareils des victimes avec des logiciels malveillants. En ce sens, cette pratique s'inscrit dans une continuité avec les méthodes de phishing traditionnelles, tout en bénéficiant d'un cadre technique plus subtil et moins immédiatement identifiable par les utilisateurs.

Dans cette optique, il est impératif de s'interroger sur le cadre juridique existant et son efficacité face à cette menace en pleine expansion. En France, comme dans d'autres pays, la législation sur la cybersécurité et la protection des données personnelles, notamment à travers le Règlement Général sur la Protection des Données (RGPD), vise à encadrer la collecte et le traitement des informations sensibles. Toutefois, la rapidité d'évolution des techniques de cybercriminalité pose la question de la capacité de ces normes à protéger efficacement les citoyens contre les nouvelles formes d'attaques, telles que le quishing.

La problématique de la responsabilité des acteurs impliqués — des concepteurs de technologies aux utilisateurs finaux — doit également être envisagée dans une perspective holistique, intégrant les dimensions éthiques et juridiques inhérentes à cette problématique. Par ailleurs, la prévention et la sensibilisation constituent des axes cruciaux dans la lutte contre le quishing. Dans un environnement où la technologie est omniprésente, il est essentiel que les utilisateurs soient formés aux risques associés à l'utilisation des codes QR et qu'ils développent des compétences critiques pour évaluer la fiabilité des informations qu'ils rencontrent. La mise en œuvre de campagnes de sensibilisation, l'instauration de bonnes pratiques en matière de sécurité numérique, ainsi que l'engagement des entreprises à garantir la sécurité de leurs systèmes

d’information sont des mesures qui pourraient contribuer à réduire l’impact de cette menace.

Enfin, il convient d’explorer les perspectives futures en matière de lutte contre le quishing, notamment à travers l’innovation technologique et l’adaptation des cadres réglementaires. À mesure que les méthodes de cybercriminalité se diversifient et se complexifient, il devient essentiel que les législateurs, les professionnels de la cybersécurité et les utilisateurs collaborent afin de bâtir un environnement numérique plus sûr. Cette synergie est d’autant plus nécessaire dans un monde où l’interconnexion croissante des systèmes amplifie les risques liés à la sécurité des données.

En somme, cette étude se propose d’explorer en profondeur la menace croissante du quishing, en analysant ses mécanismes, ses implications juridiques, et les stratégies de prévention et de protection à envisager. À travers cette analyse, nous aspirons à fournir des recommandations concrètes et pragmatiques permettant de renforcer la résilience des individus et des organisations face à cette menace insidieuse, tout en contribuant à la construction d’un cadre juridique approprié pour un avenir numérique plus sécurisé.

I- Le fonctionnement du quishing : Mécanismes et méthodes d'attaque

Le quishing, en tant que technique de cyberattaque, repose sur une méthodologie précise, qui exploite les caractéristiques des QR codes pour tromper les utilisateurs.

A- La création et la distribution des QR codes malveillants

Les cybercriminels commencent par générer un QR code qui, sous des apparences innocentes, renvoie vers une URL malveillante. Cette URL est souvent conçue pour imiter des sites légitimes, tels que des plateformes bancaires, des services de paiement en ligne ou des réseaux sociaux . La crédibilité de ces sites est renforcée par des éléments visuels familiers, rendant la fraude d'autant plus convaincante. Une fois le QR code créé, sa distribution s'effectue par divers moyens. Les canaux électroniques, tels que les courriels, les réseaux sociaux ou les applications de messagerie, sont couramment utilisés. Parallèlement, les QR codes peuvent également être placés stratégiquement sur des supports physiques, tels que des affiches dans des lieux publics, des bornes de stationnement ou des tables de restaurant. Cette omniprésence rend les utilisateurs plus enclins à scanner ces codes, souvent sans prendre le temps de réfléchir à leur provenance.

B- La redirection vers des sites malveillants : Techniques d'hameçonnage

Le quishing, ou phishing basé sur des QR codes, représente une menace croissante dans le paysage numérique actuel. En exploitant la facilité d'accès et la confiance que les utilisateurs accordent à ces codes, les cybercriminels parviennent à rediriger les victimes vers des sites malveillants. Une fois le QR code scanné, l'utilisateur est souvent conduit vers une façade trompeuse d'un site légitime, où de nombreuses techniques d'hameçonnage sont mises en œuvre.

1. Construction de sites web imitant des plateformes légitimes

Les sites malveillants sont soigneusement conçus pour ressembler à des plateformesde confiance, telles que des banques, des services de paiement ou des comptes de réseaux sociaux. Les cybercriminels investissent du temps et des ressources pour créer des copies presque parfaites de ces sites, en utilisant des logos, des couleurs et des mises en page familières. Cela augmente la probabilité que les utilisateurs, en état de confiance, fournissent leurs informations personnelles.

2. Collecte d'informations personnelles

Une fois sur un site frauduleux, l'utilisateur est souvent confronté à des formulaires lui demandant de fournir des informations sensibles. Les cybercriminels peuvent utiliser des techniques de persuasion, telles que des messages d'urgence ou des alertes de sécurité, pour inciter les utilisateurs à agir rapidement sans réfléchir. Par exemple, un message indiquant que le compte de l'utilisateur a été compromis peut le pousser à réinitialiser son mot de passe sur le site malveillant, révélant ainsi des informations critiques.

3. Téléchargement de logiciels malveillants

Dans certains cas, les sites malveillants incitent les utilisateurs à télécharger des applications ou des logiciels. Ces téléchargements peuvent contenir des logiciels espions, des chevaux de Troie ou d'autres types de malwares. Une fois installés, ces programmes peuvent accéder aux données personnelles de l'utilisateur, surveiller ses activités en ligne ou même prendre le contrôle de son appareil à distance. Cela expose non seulement l'utilisateur à des pertes financières, mais également à des atteintes à sa vie privée.

4. Techniques de manipulation psychologique

Les cybercriminels exploitent des techniques de manipulation psychologique pour maximiser l'efficacité de leurs attaques. Par exemple, ils peuvent utiliser le principe de la rareté en affirmant qu'une offre spéciale est disponible pour une durée limitée, incitant ainsi les victimes à agir rapidement. De plus, des éléments de design tels que des compteurs de temps ou des alertes de sécurité peuvent créer un sentiment d'urgence, réduisant la capacité de l'utilisateur à évaluer la situation de manière rationnelle.

5. Le rôle de la confiance et de la familiarité

La facilité avec laquelle les utilisateurs peuvent scanner des QR codes et accéder à des sites web contribue à la vulnérabilité face à ces attaques. En effet, le simple fait de scanner un code est souvent perçu comme une action anodine et sécurisée. Cette confiance aveugle dans la technologie, couplée à un manque de sensibilisation sur les méthodes utilisées par les cybercriminels, rend les utilisateurs particulièrement susceptibles aux attaques de quishing.

II- Les enjeux du quishing : Risques et mesures de prévention

Face à cette menace croissante, il est essentiel d'analyser les divers enjeux liés au quishing et d'élaborer des stratégies de prévention efficaces.

A- Les risques associés au quishing

Les conséquences d'une attaque de quishing peuvent être désastreuses, tant sur le plan individuel que collectif. Au niveau personnel, les utilisateurs ciblés peuvent subir la perte de données sensibles, comme des informations bancaires, des mots de passe ou des documents d'identité. Cette perte peut entraîner des problèmes financiers significatifs, notamment des fraudes sur des comptes bancaires ou des cartes de crédit, ainsi qu'une usurpation d'identité. Les victimes de quishing peuvent également faire face à des atteintes à leur vie privée, car les informations recueillies peuvent être utilisées à des fins malveillantes, telles que le harcèlement ou le chantage.

Les répercussions pour les entreprises sont tout aussi préoccupantes. En plus de la perte directe de données, une attaque de quishing peut entraîner une perte de confiance des clients.

Les consommateurs, de plus en plus informés des risques liés à la sécurité numérique, sont susceptibles de se détourner d'une entreprise qui ne protège pas adéquatement leurs informations personnelles. Cette perte de confiance peut se traduire par une diminution des ventes et une dégradation de la réputation de la marque. En outre, les conséquences juridiques d'une attaque de quishing peuvent être sévères. Les entreprises sont tenues de respecter des réglementations strictes en matière de protection des données, comme le Règlement Général sur la Protection des Données (RGPD) en Europe.

En cas de fuite de données sensibles, elles pourraient être exposées à des sanctions financières importantes, voire à des poursuites judiciaires. Cela peut également entraîner des audits de sécurité coûteux et une nécessité de mise en conformité rapide, impactant encore davantage les ressources de l'entreprise.

Les conséquences d'une attaque de quishing ne se limitent pas à des pertes financières immédiates. Elles peuvent également engendrer des effets à long terme sur la confiance dans les systèmes numériques. À mesure que les incidents de sécurité se multiplient, les utilisateurs peuvent devenir plus réticents à partager des informations en ligne, ce qui pourrait freiner l'innovation et la croissance dans le secteur numérique.

En fin de compte, la menace du quishing constitue un risque systémique qui affecte non seulement les individus et les entreprises, mais également l'économie numérique dans son ensemble.

B- Mesures de prévention et de protection contre le quishing

La prévention du quishing repose sur plusieurs axes, allant de la sensibilisation des utilisateurs aux mesures techniques visant à sécuriser l'accès aux QR codes.

1. Vérification des sources : L'une des premières mesures de précaution consiste à vérifier l'origine du QR code avant de le scanner. Les utilisateurs doivent être formés à reconnaître les signes d'une fraude potentielle. Par exemple, un QR code placé dans un contexte inhabituel, tel qu'une affiche sur un distributeur automatique, ou un code qui semble déplacé dans un cadre

professionnel, doit éveiller la méfiance. En cas de doute sur la légitimité d'un QR code, il est toujours préférable de ne pas le scanner.

2. Utilisation d'applications de sécurité : Plusieurs applications de scan de QR codes intègrent des fonctionnalités de sécurité qui permettent de vérifier l'URL avant de l'ouvrir. En optant pour ces outils, les utilisateurs peuvent se prémunir contre les redirections vers des sites malveillants. Il est conseillé d'utiliser des applications réputées et régulièrement mises à jour pour garantir un niveau de sécurité optimal.

3. Éducation et sensibilisation : La sensibilisation des utilisateurs est cruciale dans la lutte contre le quishing. Les entreprises et organisations doivent mettre en place des programmes de formation visant à informer leurs employés des risques liés à l'utilisation des QR codes. Des ateliers, des séminaires et des campagnes de communication peuvent contribuer à renforcer la vigilance des utilisateurs face à cette menace.

4. Mise en place de protocoles de sécurité : Les entreprises doivent également adopter des politiques de sécurité robustes concernant l'utilisation des QR codes. Cela peut inclure des vérifications régulières des codes utilisés dans le cadre de leurs opérations, ainsi que la mise en place de procédures pour signaler et gérer les incidents de quishing. De plus, il est essentiel d'intégrer des mesures de sécurité dans les systèmes d'information afin de détecter et de prévenir les accès non autorisés.

5. Suivi et mise à jour des informations : Les cybercriminels adaptent constamment leurs méthodes d'attaque, il est donc essentiel que les utilisateurs et les entreprises restent informés des dernières tendances en matière de quishing. Suivre les actualités liées à la cybersécurité et mettre à jour régulièrement les outils de protection peut aider à anticiper et à contrer les nouvelles formes d'attaques.

Sources :

1 Comment éviter l’arnaque du quishing ? (haas-avocats.com)

2 Le « quishing » : l’hameçonnage par QR code - Assistance aux victimes de cybermalveillance

3 Qu'est-ce que le quishing ? | Cloudflare

4 Cour de cassation, criminelle, Chambre criminelle, 16 février 2010, 09-81.492, Publié au bulletin - Légifrance (legifrance.gouv.fr)

5 Cour de cassation, criminelle, Chambre criminelle, 23 mai 2023, 22-86.738, Inédit - Légifrance (legifrance.gouv.fr)