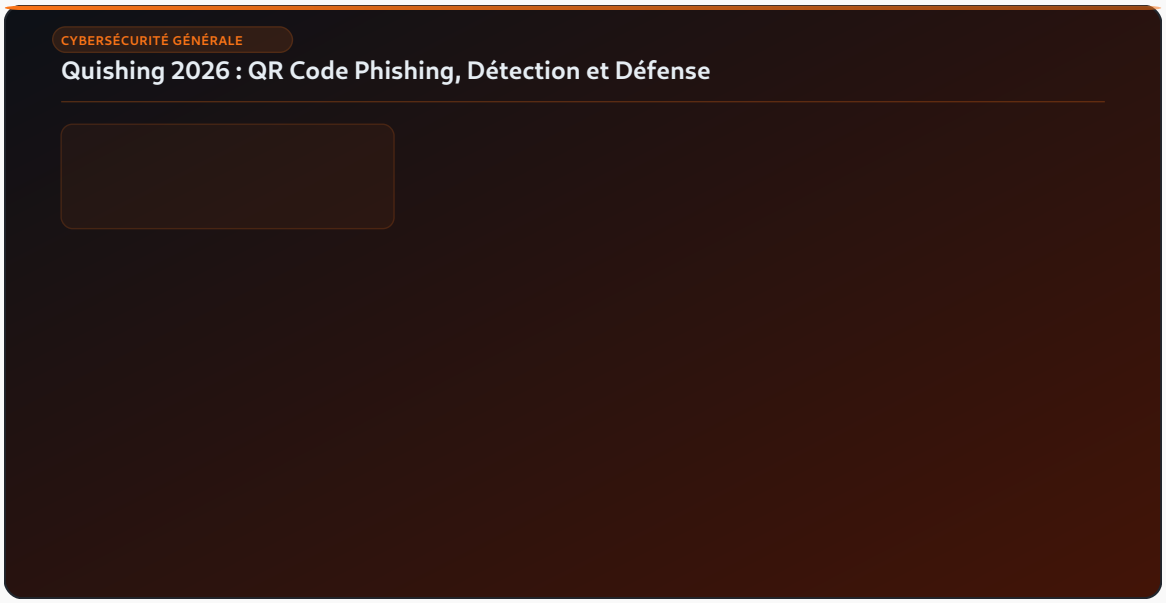
Quishing 2026 : Phishing par QR Code — Détection et Protection

> Guide complet du quishing en 2026 — phishing par QR code, techniques de camouflage, détection par email gateway et solutions de protection mobile.

Au premier semestre 2025, les équipes de threat intelligence de Proofpoint et de Microsoft ont observé une explosion des attaques de **quishing** — terme forgé de la contraction de "QR code" et "phishing" — avec une augmentation de 587% des emails contenant des QR codes malveillants par rapport à la même période en 2024. Le quishing est devenu en quelques mois l'une des techniques d'hameçonnage les plus préoccupantes pour les RSSI, et pour une raison technique très simple : la majorité des passerelles de sécurité email (email gateway, antispam, sandboxing) sont incapables d'analyser le contenu d'une image QR code intégrée dans un email. Un attaquant qui envoie un PDF contenant un QR code pointant vers une page de phishing contourne ainsi des millions d'euros d'investissement en sécurité email d'un seul coup. La France n'est pas épargnée : le CERT-FR a documenté plusieurs campagnes de quishing ciblant des entreprises françaises en 2024-2025, notamment des phishing Microsoft 365 et des fraudes bancaires distribués via QR codes dans des courriers papier et des emails. Ce guide complet analyse les techniques de quishing, les vecteurs de bypass des sécurités email, les solutions de détection disponibles et les bonnes pratiques pour protéger vos collaborateurs en mobilité.

À RETENIR



Le quishing bypasse nativement la plupart des email gateways qui n'analysent pas les images QR

Les QR codes dans les PDF, les images et les emails HTML sont les trois vecteurs principaux

L'AiTM (Adversary-in-the-Middle) via QR code permet de contourner le MFA et voler les sessions

Microsoft Defender for Office 365 Plan 2 et Proofpoint TAP ont intégré la décodification QR en 2024

La formation utilisateurs doit inclure la règle : jamais scanner un QR code reçu par email sans vérification

Anatomie du Quishing : Comment l'Attaque Fonctionne

Le quishing exploite une lacune fondamentale des systèmes de sécurité email : leur traitement différencié entre le contenu textuel (analysé) et les images (souvent ignorées ou analysées superficiellement). Un QR code est une image contenant une URL encodée ; la plupart des systèmes de filtrage email scrutent les URLs dans le texte et dans les attributs href HTML, mais ne décodent pas les images QR pour en extraire les URLs potentiellement malveillantes.

> ⚡ **Retour terrain**
>
> J'ai conduit une campagne de phishing simulé pour un cabinet juridique de 80 personnes. Premier envoi : 61 % de taux de clic. Après une session de sensibilisation de 90 minutes : 34 % au second envoi six semaines plus tard. La leçon inattendue : les associés (les profils les plus sensibles aux simulations de fausses factures) avaient un taux de clic 2× plus élevé que les secrétaires — à l'inverse de ce que l'équipe RH anticipait.

Vecteur 1 — QR code dans le corps de l'email HTML : le plus simple. L'attaquant insère une image QR code encodant une URL malveillante directement dans le corps HTML de l'email. Visuellement, l'email ressemble à une communication légitime (notification de sécurité Microsoft, alerte bancaire, invitation à une réunion Teams) et demande au destinataire de scanner le QR code avec son smartphone "pour plus de sécurité" ou "parce que le lien email pose des problèmes".

Vecteur 2 — QR code dans une pièce jointe PDF : plus sophistiqué. Le PDF contient un QR code sur une ou plusieurs pages. Ce vecteur est particulièrement efficace car les PDFs joints sont souvent considérés comme plus légitimes que les URLs directes par les utilisateurs, et les systèmes de sandboxing de PDF doivent ouvrir et analyser le document pour découvrir le QR code. Si le sandboxing ne supporte pas la décodification QR dans les PDFs, le contenu malveillant passe inaperçu.

Vecteur 3 — QR code physique : des campagnes documentées en 2024-2025 ont distribué des QR codes malveillants via courrier postal (faux avis de colis, faux avis d'imposition) ou via des affichettes collées sur des équipements publics (parkings payants, bornes de recharge électrique). Ce vecteur physique échappe totalement aux systèmes de sécurité email et ne peut être contré que par la sensibilisation des utilisateurs.

Techniques de Camouflage QR Code : Art de l'Évasion

Les attaquants ont développé des techniques d'évasion spécifiques pour contrer les email gateways qui commencent à implémenter la décodification QR. Ces techniques évoluent rapidement et les défenseurs doivent s'adapter en conséquence.

Segmentation du QR code : l'image QR est découpée en plusieurs fragments disposés dans un tableau HTML. Chaque fragment est une image séparée, aucune ne contient de QR code valide individuellement. Le navigateur les assemble à l'affichage, recréant un QR code lisible par le scanner du smartphone, mais les analyseurs d'images qui traitent les images individuellement ne peuvent pas détecter la menace.

QR code intégré dans une image plus grande : le QR code est intégré dans une image de fond plus large (logo d'entreprise, bannière marketing), ce qui rend la détection algorithmique plus difficile. Des systèmes de détection naïfs recherchent des images QR autonomes et ratent les QR codes intégrés dans des composites.

Obfuscation par bruit visuel : du bruit visuel léger est ajouté à l'image QR pour tromper les algorithmes de détection tout en restant lisible par les scanners QR des smartphones modernes (qui ont une bonne tolérance aux erreurs grâce à la correction d'erreurs Reed-Solomon intégrée dans le standard QR).

Techniques d'évasion QR documentées en 2025

QR code Unicode : construction du QR code avec des caractères Unicode pleins (▀, ▄, ▄) au lieu d'une image — bypass complet des analyseurs d'images

QR code ASCII art : représentation textuelle du QR code, invisible pour les analyseurs d'images mais lisible par certains scanners

QR code SVG : encodage du QR code en SVG inline dans le HTML — analysé différemment des images PNG/JPG

Redirections étagées : le QR code pointe vers un domaine légitime (Google Forms, OneDrive) qui redirige ensuite vers la page de phishing

QR dynamique : le QR code pointe vers un service de raccourcissement d'URL dont la destination change après quelques scans

AiTM via QR Code : Contournement du MFA

L'utilisation des QR codes comme vecteur d'attaques AiTM (Adversary-in-the-Middle) est une évolution particulièrement dangereuse observée depuis mi-2024. Cette technique combine le bypass de l'email gateway (QR code non analysé) avec le contournement du MFA (proxy AiTM en temps réel).

Le flux d'attaque est le suivant : l'email de quishing contient un QR code pointant non pas directement vers une fausse page de connexion, mais vers un proxy AiTM (Evilginx3, Modlishka). L'utilisateur qui scanne le QR avec son smartphone est redirigé vers une page de connexion Microsoft 365 qui semble identique à l'originale — c'est en réalité un proxy transparent qui intercepte la session TLS entre le smartphone et les serveurs Microsoft. Lorsque l'utilisateur saisit ses identifiants et valide son MFA (approbation Teams ou code OTP), le proxy

intercepte le cookie de session authentifiée et le transmet à l'attaquant en temps réel. L'attaquant dispose alors d'un accès complet à la boîte Microsoft 365 de la victime, **malgré le MFA**.

Cette attaque est particulièrement efficace sur les smartphones qui sont la cible naturelle du quishing : l'URL visible dans le navigateur mobile est souvent tronquée, la vérification du certificat HTTPS est plus difficile sur un petit écran, et les utilisateurs sont moins méfiants lorsqu'ils scannent un QR code que lorsqu'ils cliquent sur un lien.

Technique	Bypass email gateway	Bypass MFA	Sophistication
QR code HTML basique	Souvent (gateway sans décodage QR)	Non	Faible
QR dans PDF	Généralement (sandboxing incomplet)	Non	Moyenne
QR segmenté	Presque toujours	Non	Haute
QR + AiTM proxy	Presque toujours	Oui (bypass complet)	Très haute

Détection par Email Gateway : Solutions et Limites

Depuis 2024, les principales solutions de sécurité email ont intégré des capacités de décodification QR pour contrer le quishing. Voici l'état des capacités des principales solutions du marché français.

Microsoft Defender for Office 365 Plan 2 (anciennement ATP) : décodification QR intégrée depuis septembre 2023 dans les filtres anti-phishing. Les emails contenant des QR codes sont détonés dans un sandbox, l'URL extraite est vérifiée contre Microsoft Threat Intelligence et les listes de réseaux sûrs. Le Plan 1 (inclus dans M365 Business Premium) a des capacités plus limitées sur la détonation des QR codes. Résultat terrain : efficace à ~85% sur les QR codes HTML directs, moins efficace sur les QR codes segmentés.

Proofpoint Targeted Attack Protection (TAP) : l'une des premières solutions à avoir intégré la décodification QR en production (depuis fin 2023). Proofpoint utilise une approche multi-moteurs : OCR pour extraire les URLs des images QR, analyse comportementale de la

destination, et intelligence sur les domaines malveillants. Efficacité annoncée : >90% de détection sur les vecteurs connus.

Mimecast CTP (Cyber Threat Protection) : décodification QR et analysis URL disponibles depuis début 2024. Intègre aussi la protection contre les QR codes dans les pièces jointes PDF. **Abnormal Security** : approche comportementale qui flag les emails contenant des QR codes envoyés depuis des expéditeurs inhabituels ou des domaines récemment enregistrés.

MDM et Contrôle de la Caméra : Protection Côté Terminal

La protection contre le quishing au niveau du terminal mobile est une approche complémentaire aux défenses email. Si l'email gateway ne peut pas détecter le QR code malveillant, empêcher le smartphone de scanner le QR code est la dernière ligne de défense.

Les solutions MDM (Mobile Device Management) comme Microsoft Intune, Jamf Pro, ou VMware Workspace ONE permettent de déployer des politiques qui restreignent l'accès à l'application caméra native ou forcent l'utilisation d'un scanner QR approuvé par l'entreprise. Un scanner QR "corporate" peut être configuré pour vérifier l'URL extraite contre une liste de domaines autorisés (allowlist) ou une liste de domaines malveillants connus (blocklist) avant d'ouvrir le navigateur.

Microsoft Intune avec la politique App Protection Policy (APP) permet également de forcer l'ouverture des URLs issues de QR codes dans Microsoft Edge (Intune-managed) plutôt que dans le navigateur par défaut. Edge Intune-managed bénéficie de la protection contre les sites de phishing via Microsoft SmartScreen, ce qui ajoute une couche de protection même après le scan du QR code malveillant.

Quishing Physique : Bornes de Recharge et Affichettes

Le quishing physique — QR codes malveillants collés sur des équipements publics ou distribués par courrier postal — est un vecteur que les entreprises françaises doivent inclure dans leurs programmes de sensibilisation. Ce vecteur a connu une expansion significative en France en 2024-2025, documentée par plusieurs services de police et de gendarmerie.

Les cibles les plus fréquentes des QR codes malveillants physiques : **bornes de recharge électrique** (QR code malveillant sur le sticker de la borne, promettant un accès à l'application de paiement), **horodateurs de stationnement** (QR code promettant un paiement facilité), **menus de restaurant** (QR code remplacé par un QR code malveillant promettant une commande en ligne), et **courriers officiels frauduleux** (faux avis d'amende, faux avis URSSAF ou CAF contenant un QR code de "paiement").

La règle de formation fondamentale contre le quishing physique est simple : **ne jamais scanner un QR code sur un équipement public sans vérifier visuellement que le sticker n'est pas collé par-dessus un QR code d'origine**. Sur les bornes de recharge, vérifier que l'URL affichée après scan correspond au domaine officiel de l'opérateur (IONITY, Lidl Charge, Electra, etc.).

Campagnes de Quishing Documentées en France 2024-2025

L'analyse des campagnes de quishing ayant ciblé la France permet d'identifier des patterns récurrents utiles pour la formation des utilisateurs.

Campagne Microsoft 365 Q3 2024 : emails prétendant provenir de Microsoft Security Team, demandant de scanner un QR code pour "sécuriser son compte" ou "valider son accès MFA". Le QR code pointait vers un proxy AiTM imitant la page de connexion Microsoft. Plusieurs centaines d'entreprises françaises ont été ciblées selon Proofpoint France. Indicateurs : emails avec objets "Action requise : sécurisation de votre compte Microsoft", domaines de redirection enregistrés dans les 48h précédant l'envoi.

Campagne phishing bancaire via courrier Q4 2024 : courriers physiques usurpant l'identité de BNP Paribas, Crédit Agricole et Société Générale, avec QR codes demandant de "valider son

RIB" ou "mettre à jour ses coordonnées bancaires". La CERT-FR et Cybermalveillance.gouv.fr ont publié des alertes communes sur cette campagne. Les victimes étaient principalement des particuliers et des travailleurs indépendants.

Anecdote terrain : le QR code de la borne de recharge

En décembre 2024, un commercial d'une PME lyonnaise utilise une borne de recharge Electra dans un parking de centre commercial. Il scanne le QR code sur la borne pour payer via l'application. La page de "paiement" lui demande ses identifiants de carte bancaire et son code 3D Secure. Il les saisit, sa carte est débitée de 1 euro "pour vérification", et 48h plus tard, il constate 3 transactions frauduleuses pour un total de 2 800 euros. Un sticker avec un QR code malveillant avait été collé sur le QR code Electra d'origine. Lors de l'enquête, les traces de colle du sticker malveillant étaient encore visibles sur 7 bornes du même parking.

Formation Utilisateurs au Quishing : Contenu et Métriques

La formation des utilisateurs au quishing doit intégrer des éléments spécifiques qui ne sont pas couverts par les formations phishing traditionnelles. Le comportement à adopter face à un QR code reçu par email est contre-intuitif pour beaucoup d'utilisateurs habitués à scanner des QR codes dans leur vie quotidienne (restaurants, transports, événements).

Les messages clés à transmettre lors des formations : (1) **un QR code dans un email est intrinsèquement suspect** — les communications légitimes fournissent des liens texte cliquables, pas des QR codes ; (2) scanner un QR code avec son smartphone personnel contourne les protections de sécurité du poste de travail professionnel ; (3) **vérifier toujours l'URL affichée par le scanner avant d'ouvrir** — si l'URL ne correspond pas au domaine attendu, ne pas

continuer ; (4) pour les QR codes physiques sur des équipements, vérifier visuellement l'intégrité du sticker.

Intégration du Quishing dans le SOC : Règles de Détection

Le SOC doit disposer de règles de détection spécifiques au quishing pour identifier les incidents en cours ou les tentatives passées. La difficulté est que les QR codes malveillants sont souvent scannés depuis des smartphones personnels ou MDM qui ne remontent pas de logs vers le SOC d'entreprise.

Les règles de détection pertinentes côté email (Microsoft 365 Defender / Exchange Online) : alerter sur les emails contenant des images sans texte associé (rapport image/texte anormalement élevé), les emails avec des images à haute densité de pixels noirs sur fond blanc dans une zone centrale (signature visuelle d'un QR code), et les emails qui ont déclenché des analyses d'URLs suspectes après décodification QR par le gateway.

Côté réseau, si des proxies web centralisent les accès Internet des smartphones MDM, les connexions vers des domaines enregistrés depuis moins de 30 jours depuis des appareils mobiles professionnels après les heures habituelles de bureau peuvent signaler une tentative de quishing ayant réussi à tromper l'utilisateur.

Cadre Réglementaire : Quishing et Obligations CNIL/NIS 2

Un incident de quishing réussi entraînant un accès non autorisé à des boîtes email d'entreprise ou des systèmes d'information constitue une violation de données personnelles au sens du RGPD si des données personnelles sont exposées. La notification à la CNIL dans les 72 heures (article 33 RGPD) est obligatoire si l'incident présente un risque pour les droits et libertés des personnes concernées.

Pour les entités soumises à NIS 2, un incident de quishing ayant conduit à une compromission de systèmes d'information essentiels doit être déclaré à l'ANSSI dans les 24 heures (rapport initial) et 72 heures (rapport intermédiaire). La notification précoce est obligatoire même si l'évaluation complète de l'impact n'est pas encore disponible. L'ANSSI a publié des guides pratiques sur les obligations de notification qui précisent les critères de déclenchement pour les incidents de type phishing/quishing.

Liens Complémentaires et Ressources

Pour approfondir la protection contre le phishing en général et les variantes email, consultez notre guide complet sur DMARC, DKIM, SPF et BIMI 2026 et notre article sur le BEC et vishing augmentés par l'IA. Pour les aspects de protection des appareils mobiles via MDM, notre guide sur la sécurisation des accès Microsoft 365 avec MFA couvre Intune et les politiques d'accès conditionnel. Le rapport Proofpoint State of the Phish 2025 sur le quishing est disponible sur proofpoint.com. L'alerte CERT-FR sur les arnaques au QR code est disponible sur cybermalveillance.gouv.fr.

Quishing et Systèmes MFA Résistants au Phishing

La réponse structurelle au quishing AiTM est le déploiement de méthodes MFA résistantes au phishing qui ne peuvent pas être interceptées par un proxy AiTM, même si l'utilisateur a été trompé par un QR code malveillant. Ces méthodes MFA "phishing-resistant" sont recommandées par la CISA, le NIST et l'ANSSI pour les accès les plus sensibles.

FIDO2/WebAuthn avec clés matérielles (YubiKey, Titan Key) : la validation est liée cryptographiquement à l'URL du site légitime. Un proxy AiTM ne peut pas intercepter la validation FIDO2 car la clé matérielle signe un challenge spécifique à l'origine (origin binding) — si l'URL du proxy est différente de l'URL légitime, la validation échoue automatiquement. C'est la méthode la plus robuste contre le quishing AiTM.

Microsoft Authenticator avec correspondance de numéros (Number Matching) : introduit en 2023, force l'utilisateur à saisir un code affiché dans le contexte de connexion dans l'application Authenticator. Moins robuste que FIDO2 mais significativement plus résistant que les approbations MFA push classiques qui peuvent être fatiguées (MFA fatigue attacks). Pour les comptes Microsoft 365, la politique "Authentication Strength" peut forcer l'utilisation de méthodes résistantes au phishing dans les politiques d'Accès Conditionnel.

Tableau de Bord RSSI : KPI Anti-Quishing

Pour piloter la protection contre le quishing, voici les indicateurs à suivre dans le tableau de bord RSSI mensuel.

KPI	Mesure	Cible	Source
Emails QR bloqués	Nb emails avec QR code malveillant détectés/ bloqués	Tendance	Email gateway
Taux signalement quishing	% employés signalant emails QR suspects au SOC	>60%	Simulation trimestrielle
Couverture MFA résistant	% comptes sensibles avec MFA phishing-resistant	>80%	Azure AD / Entra ID
MDM smartphones	% smartphones pro enrôlés MDM avec policy QR	>95%	Intune / Jamf

Quishing et Gestion des Voyageurs d'Affaires

Les voyageurs d'affaires constituent une cible de choix pour les campagnes de quishing physique en raison de leur exposition accrue aux QR codes dans les environnements hôteliers, aéroportuaires et de transport. Un employé en déplacement est souvent plus pressé, moins attentif aux détails de sécurité, et utilise son smartphone pour accéder aux systèmes d'information

de l'entreprise depuis des réseaux Wi-Fi non sécurisés — une combinaison particulièrement risquée.

Les vecteurs de quishing spécifiques aux voyageurs d'affaires : **QR codes de connexion Wi-Fi hôtel** (QR malveillant sur la carte de bienvenue ou le panneau d'accueil), **QR codes de menus restaurant** dans les halls d'hôtel et salons d'affaires, **QR codes de bornes d'enregistrement ou de self check-in**, et **QR codes dans les salles de conférence** pour partager des documents ou accéder au réseau de présentation. Ces vecteurs sont d'autant plus dangereux que le voyageur scannerait les QR codes légitimes dans ces mêmes contextes — la distinction est difficile.

La politique de sécurité des voyageurs doit inclure : interdiction de scanner des QR codes pour se connecter au Wi-Fi d'hébergement (utiliser le code Wi-Fi textuel fourni par la réception), utilisation systématique d'un VPN sur les réseaux externes, et formation spécifique aux risques de quishing dans les déplacements professionnels. Le **programme IATA Cybersecurity in Aviation** inclut des recommandations spécifiques sur les QR codes pour les personnels navigants.

Gouvernance de la Protection Anti-Quishing

La gouvernance anti-quishing doit être intégrée dans le programme global de cybersécurité de l'organisation, avec des responsabilités clairement définies et des processus de revue réguliers.

Le **RSSI** est responsable de la stratégie globale anti-quishing : choix des solutions techniques, définition des politiques MDM, supervision des programmes de formation, et reporting au COMEX. Le **responsable email/messagerie** (souvent dans la DSI) est responsable de la configuration et de la maintenance des solutions de protection email incluant la décodification QR. Le **responsable formation** (souvent en RH ou DSI) est responsable de l'intégration du quishing dans les programmes de sensibilisation et des simulations périodiques.

Un **comité de revue trimestrielle** réunissant RSSI, DSI et directions métier (finance, RH, achats) permet de suivre les métriques anti-quishing, d'analyser les incidents récents, et d'adapter les mesures aux nouvelles techniques observées. Ce comité doit également maintenir à jour la

politique de signalement des emails suspects pour s'assurer que les QR codes malveillants détectés par les utilisateurs remontent systématiquement au SOC.

L'Avenir du Quishing : Tendances 2026-2027

La menace quishing va continuer d'évoluer dans les prochains mois sous l'impulsion de plusieurs facteurs : l'amélioration des techniques d'évasion QR, l'intégration du quishing dans des campagnes multi-vecteurs sophistiquées, et l'exploitation de nouveaux contextes (réseaux sociaux, applications métier, communications internes d'entreprise).

Une tendance émergente est le **quishing via les systèmes de collaboration interne** : Microsoft Teams, Slack et Zoom permettent de partager des images directement dans les channels. Un attaquant qui a compromis un compte interne peut distribuer des QR codes malveillants dans les channels de messagerie interne, bénéficiant de la confiance implicite accordée aux communications entre collègues. Les solutions de protection DLP (Data Loss Prevention) sur ces plateformes commencent à intégrer la détection QR dans leur périmètre d'analyse.

L'intégration du quishing dans les attaques de **supply chain logicielle** est une autre tendance à surveiller : des packages npm/PyPI malveillants qui affichent un QR code dans leur README GitHub ou leur documentation, invitant les développeurs à scanner pour "valider leur licence" ou "accéder à la documentation avancée". Ce vecteur cible spécifiquement les équipes de développement, population à forte valeur pour les attaquants.

Du côté défensif, l'intégration des capacités de détection quishing dans les plateformes XDR (Extended Detection and Response) va permettre une corrélation plus efficace entre les tentatives de quishing email et les comportements suspects post-scan sur les endpoints mobiles. Microsoft Defender XDR, CrowdStrike Falcon XDR et Palo Alto Cortex XDR ont tous des roadmaps qui incluent cette corrélation mobile-email pour 2026-2027.

Mon Opinion sur la Menace Quishing

Le quishing illustre parfaitement un problème récurrent en sécurité : les défenseurs construisent des protections sophistiquées contre les menaces connues (URLs malveillantes dans le texte email, phishing pages avec certificats invalides, domaines connus malveillants), et les attaquants contournent ces protections en changeant simplement le vecteur d'entrée. Un QR code encode une URL exactement comme un lien href, mais la protection en place ignore le QR code. C'est fondamentalement une question d'angle mort.

La vraie solution au quishing n'est pas uniquement technique : c'est une combinaison de formation utilisateurs pour changer le comportement face aux QR codes, de protection MFA résistante au phishing qui rend le vol de session inopérant même si l'utilisateur est trompé, et de détection QR dans les email gateways pour bloquer le vecteur principal. Ces trois éléments doivent être déployés ensemble pour une protection efficace.

Plan d'Action Anti-Quishing : Priorités Opérationnelles

Voici un plan d'action structuré pour renforcer la protection anti-quishing dans les 90 prochains jours, organisé par priorité et par effort requis.

Semaines 1-2 (impact immédiat) : vérifier que votre solution de protection email décode les QR codes (contacter votre éditeur et tester avec un email de test) ; envoyer une communication de sensibilisation rapide aux équipes ciblées (finance, RH, direction) expliquant le risque quishing et la règle "jamais scanner un QR code reçu par email sans validation" ; et auditer la couverture MFA sur les comptes à privilèges pour identifier les comptes encore sans MFA phishing-resistant.

Semaines 3-6 (consolidation) : si votre email gateway ne décode pas les QR codes, évaluer une mise à niveau ou un ajout de couche (Defender for Office 365 P2, ajout d'une couche Proofpoint/ Mimecast) ; configurer les politiques MDM pour forcer l'utilisation d'un scanner QR corporate sur les smartphones professionnels ; et déployer une campagne de simulation quishing pour mesurer le taux de comportement à risque dans votre organisation.

Semaines 7-12 (maturité) : déployer des clés FIDO2 ou activer le Number Matching MFA sur tous les comptes admin et direction ; intégrer les règles de détection quishing dans le SIEM ; et établir un reporting mensuel KPI anti-quishing pour le RSSI et le COMEX.

Quishing dans les Environnements B2B : Risques Spécifiques

Les environnements B2B présentent des vecteurs de quishing spécifiques que les environnements grand public ne connaissent pas. Les factures électroniques, les bons de commande, les documents contractuels et les communications entre entreprises partenaires constituent des vecteurs d'attaque privilégiés car ils jouissent d'une présomption de légitimité plus forte que les emails grand public.

Un scénario d'attaque B2B fréquent : un attaquant compromise la boîte email d'un fournisseur (via phishing classique), puis envoie depuis cette boîte légitime une facture PDF à tous les clients du fournisseur. La facture PDF contient un QR code sur la page de paiement, invitant à scanner pour "accéder au portail de paiement en ligne". La boîte légitime du fournisseur contourne tous les filtres de réputation email. Seule la décodification QR et la vérification de l'URL extraite peuvent bloquer cet attack.

Les plateformes d'e-procurement (Coupa, SAP Ariba, Ivalua) sont également des cibles potentielles : un attaquant qui compromise un compte fournisseur sur ces plateformes peut soumettre des documents contenant des QR codes dans l'interface de la plateforme elle-même, ciblant les acheteurs qui consultent les documents via l'application web de la plateforme.

Technologies Anti-Quishing Émergentes en 2026

L'écosystème des solutions anti-quishing évolue rapidement pour répondre à la sophistication croissante des attaques. Plusieurs approches technologiques émergentes méritent l'attention des RSSI en 2026.

Browser Isolation pour les smartphones : des solutions comme Lookout (anciennement MobileIron Threat Defense) ou Jamf Protect permettent d'ouvrir automatiquement les URLs issues de QR codes dans un navigateur isolé en sandbox cloud. La page de phishing se charge dans le cloud et l'utilisateur voit un rendu sécurisé sans que son smartphone n'interagisse directement avec le serveur malveillant. Cette approche est particulièrement efficace contre les sites de phishing qui détectent les sandbox et affichent un contenu inoffensif dans ces environnements.

DNS Filtering sur mobile : des solutions comme Cisco Umbrella Mobile, Cloudflare Gateway ou NextDNS en mode enterprise peuvent filtrer les requêtes DNS depuis les smartphones MDM, bloquant les accès vers des domaines malveillants même lorsque l'utilisateur a scanné un QR code. L'efficacité dépend de la couverture des listes de domaines malveillants et de la latence entre l'enregistrement du domaine et son ajout aux listes de filtrage.

URL reputation en temps réel dans les applications scanner : des applications de scan QR "enterprise" comme **QR & Barcode Scanner Pro** (avec intégration VirusTotal) ou des applications MDM custom peuvent vérifier l'URL extraite contre des API de réputation en temps réel (VirusTotal, URLhaus, Google Safe Browsing) avant de l'ouvrir dans le navigateur. Cette approche offre une protection côté terminal qui complète les défenses côté email gateway.

Quishing et Réseaux Sociaux : Nouvelle Surface d'Attaque

Les réseaux sociaux professionnels (LinkedIn) et grand public (Instagram, TikTok, X/Twitter) sont devenus des vecteurs de distribution de QR codes malveillants. Des profils faux imitant des marques connues (banques, services gouvernementaux, grandes entreprises) publient des posts avec des QR codes promettant des offres spéciales, des remboursements d'impôts ou des concours.

Sur **LinkedIn**, des posts de type "Recevez notre livre blanc gratuit en scannant ce QR code" constituent un vecteur de quishing crédible dans un contexte professionnel. La légitimité apparente du contenu (livre blanc, étude sectorielle) et la confiance accordée aux contenus LinkedIn dans un contexte business rendent les employés moins méfiants que face à un email similaire.

La protection contre le quishing via les réseaux sociaux repose essentiellement sur la sensibilisation : former les employés à ne jamais scanner de QR code dans un post de réseau social sans vérifier l'identité de l'émetteur (vérification du profil, de son historique, du nombre de followers) et sans vérifier l'URL affichée après scan. Les solutions MDM peuvent aussi bloquer les navigateurs ouverts depuis des applications de réseaux sociaux sur les smartphones professionnels.

Statistiques et Benchmarks Quishing 2025

Pour contextualiser l'ampleur de la menace quishing, voici les données chiffrées disponibles dans les rapports sectoriels 2025.

Statistique	Valeur	Source
Croissance emails quishing H1 2025 vs H1 2024	+587%	Proofpoint
% emails phishing contenant un QR code (Q2 2025)	17%	Checkpoint
Taux de clic sur QR codes malveillants (simulation)	32%	KnowBe4
% gateways email avec décodage QR actif	43%	Gartner 2025
Pertes quishing estimées France 2024	>50M€	CERT-FR estimation

Collaboration avec les Éditeurs : Signalement des QR Codes Malveillants

Le signalement rapide des QR codes malveillants aux éditeurs de sécurité et aux autorités permet d'accélérer la mise en liste noire des domaines ciblés et de protéger d'autres potentielles victimes. En France, plusieurs canaux de signalement sont disponibles.

Phishing Initiative (phishing-initiative.fr) permet de signaler des URLs de phishing qui sont ensuite transmises aux principaux filtres de sécurité (Google Safe Browsing, Microsoft SmartScreen, Mozilla). Les URLs extraites de QR codes malveillants peuvent être signalées via ce service. **Internet Signalement** (internet-signalement.fr) de l'OCLTIC (Office Central de Lutte contre la criminalité liée aux Technologies de l'Information et de la Communication) permet de signaler les contenus illicites incluant les sites de phishing.

Pour les entreprises, le signalement via les portails dédiés des éditeurs de sécurité email (Microsoft Defender Submission Portal, Proofpoint Threat Submission) permet d'enrichir directement les bases de renseignement utilisées pour protéger tous les clients de ces solutions. Ce signalement est une responsabilité collective qui améliore la protection de l'écosystème global.

Checklist Technique Anti-Quishing pour les Équipes Sécurité

Pour les équipes de sécurité qui souhaitent auditer rapidement leur posture anti-quishing, voici une checklist technique organisée par domaine.

Email Gateway : vérifier que la décodification QR est activée dans les paramètres de la solution ; confirmer que les PDFs et les images sont scannés pour les QR codes et pas seulement pour les malwares ; tester avec un email de simulation contenant un QR code ; vérifier les paramètres de sandboxing pour les pièces jointes PDF.

Microsoft 365 / Entra ID : vérifier que les politiques d'Accès Conditionnel exigent un MFA phishing-resistant pour les accès depuis des appareils non-conformes (smartphones non-MDM) ; activer le Number Matching sur Microsoft Authenticator pour tous les utilisateurs ; configurer les règles Anti-Phishing dans Defender for Office 365 pour les emails avec pièces jointes PDF.

MDM (Intune/Jamf) : vérifier que tous les smartphones professionnels sont enrôlés ; configurer une application de scan QR corporate avec vérification URL ; bloquer l'ouverture de navigateurs non-gérés depuis les applications de scan QR natif si possible ; activer les notifications de conformité pour les appareils non-enrôlés. Notre guide Zero Trust Microsoft 365 détaille la configuration Intune pour les appareils mobiles.

Aspects Juridiques des Attaques Quishing en France

Les attaques quishing constituent en droit français plusieurs infractions pénales selon la nature de l'action et les préjudices causés. Comprendre le cadre juridique aide les organisations à formuler correctement les plaintes et à identifier les recours disponibles.

L'**escroquerie** (article 313-1 du Code pénal) est l'infraction principale retenue pour les attaques quishing qui conduisent à des virements frauduleux ou à la divulgation de données bancaires. L'escroquerie est punie de 5 ans d'emprisonnement et 375 000 euros d'amende (aggravée en bande organisée). L'**accès frauduleux à un système de traitement automatisé de données** (article 323-1 du Code pénal) est retenu lorsque le quishing conduit à une compromission de compte et à un accès non autorisé aux systèmes d'information de la victime. Peine maximale : 3 ans d'emprisonnement et 100 000 euros d'amende, aggravée à 5 ans et 150 000 euros si des données ont été modifiées.

La victime d'une attaque quishing en France dispose de plusieurs voies de recours : dépôt de plainte à la brigade cybercriminalité (C3N ou OCLTIC selon le niveau de l'attaque), signalement sur internet-signalement.fr, et demande de mesures conservatoires d'urgence (gel des avoirs via les procédures d'entraide judiciaire internationale). L'assistance d'un avocat spécialisé en droit numérique est recommandée pour les attaques dépassant 50 000 euros afin d'optimiser les chances de recouvrement.

Synthèse : Matrice de Maturité Anti-Quishing

Pour évaluer rapidement la maturité de votre organisation face au quishing, utilisez cette matrice d'évaluation en 5 dimensions clés. Chaque dimension est notée de 1 (inexistant) à 4 (optimal).

Dimension 1 — Détection email : 1=pas de détection QR ; 2=détection QR basique sans sandbox PDF ; 3=détection QR avec sandbox PDF et analyse comportementale ; 4=détection QR multi-format (HTML, PDF, SVG, Unicode) avec threat intelligence intégrée.

Dimension 2 — Protection MFA : 1=SMS OTP ou pas de MFA ; 2=Authenticator app push ; 3=Number Matching activé ; 4=FIDO2/Passkeys phishing-resistant sur tous les comptes.

Dimension 3 — MDM Mobile : 1=aucun MDM ; 2=MDM partiel (smartphones perso non gérés) ; 3=MDM complet avec scanner QR corporate ; 4=MDM complet + browser isolation + DNS filtering mobile.

Dimension 4 — Formation : 1=aucune formation spécifique quishing ; 2=sensibilisation ponctuelle ; 3=simulation quishing annuelle avec métriques ; 4=programme continu avec simulations trimestrielles et modules e-learning adaptifs.

Dimension 5 — Réponse à incident : 1=aucune procédure ; 2=procédure ad hoc ; 3=procédure documentée avec contacts identifiés ; 4=procédure testée avec runbooks SOC spécifiques quishing et contacts bancaires préétablis pour recall SEPA.

Comparatif des Solutions Anti-Quishing du Marché

Pour aider les RSSI à choisir la solution la plus adaptée à leur contexte, voici un comparatif structuré des principales solutions disponibles sur le marché français en 2026, avec leurs forces et limites spécifiques sur le quishing.

Microsoft Defender for Office 365 Plan 2 est le choix naturel pour les organisations full Microsoft 365. La décodification QR est intégrée depuis 2023 et s'améliore régulièrement. Son principal avantage est l'intégration native avec l'écosystème M365 (Sentinel, Intune, Entra ID) pour une réponse corrélée. Limitation : moins efficace sur les QR codes segmentés et les techniques d'évasion avancées que les solutions dédiées.

Proofpoint Targeted Attack Protection est la solution la plus complète sur le marché pour la détection des menaces email avancées, incluant le quishing. Son approche multi-moteurs et sa riche threat intelligence la placent en tête des benchmarks indépendants (SE Labs, Opus One). Limitation : coût élevé et nécessite une expertise pour une configuration optimale.

Abnormal Security excelle sur les approches comportementales qui complètent (plutôt que remplacent) la décodification QR. Son analyse du comportement habituel des correspondants est particulièrement efficace pour détecter les QR codes envoyés depuis des contextes inhabituels. Limitation : moins efficace contre les QR codes envoyés depuis des expéditeurs "normaux" (supply chain compromise).

Mon opinion sur cette comparaison : pour une ETI française avec budget limité, la combinaison Microsoft Defender for Office 365 Plan 2 (inclus dans Microsoft 365 E3/E5 ou Business Premium) + Intune MDM (inclus dans E3) offre un rapport qualité-prix excellent et couvre l'essentiel des vecteurs de quishing courants. Pour les organisations avec des besoins de protection plus élevés (secteurs régulés, OIV, grandes entreprises), l'ajout d'une solution spécialisée comme Proofpoint ou Abnormal Security en couche complémentaire justifie l'investissement supplémentaire.

FAQ — Questions sur le Quishing

Pourquoi les filtres email ne bloquent-ils pas les QR codes malveillants ?

Historiquement, les filtres email analysent le contenu textuel et les URLs dans le HTML. Les images sont analysées pour des malwares mais pas décodifiées pour en extraire le contenu QR. C'est une lacune connue que les éditeurs corrigent progressivement depuis 2023-2024. Si votre solution email n'a pas été mise à jour depuis 2022, elle est probablement aveugle aux QR codes malveillants.

Est-ce qu'un QR code HTTPS protège contre le quishing ?

Non. HTTPS garantit que la communication entre le navigateur et le serveur est chiffrée, pas que le serveur est légitime. Les sites de phishing utilisent quasi-systématiquement HTTPS avec des certificats Let's Encrypt valides depuis 2019. Un cadenas vert dans la barre d'adresse ne signifie pas que le site est digne de confiance — il signifie seulement que la connexion est chiffrée.

Les QR codes reçus par SMS sont-ils aussi dangereux ?

Les SMS contiennent des URLs textuelles, pas des QR codes (les images ne s'affichent pas dans les SMS standards). Le smishing (SMS phishing) utilise des URLs raccourcies ou des URLs directes. En revanche, les SMS peuvent demander à l'utilisateur de scanner un QR code montré

sur une image séparée ou de se rendre à une URL pour "scanner un code" — des variantes du quishing qui méritent la même méfiance.

Comment tester si notre email gateway détecte les QR codes malveillants ?

Créez un QR code pointant vers un domaine de test connu comme malveillant (par exemple un domaine dans les listes de phishing publiques) via un générateur QR code en ligne, intégrez-le dans un email de test, et envoyez-le vers votre adresse d'entreprise. Si l'email passe et que le QR code s'affiche sans alerte, votre gateway ne décode pas les QR codes. Ne testez que sur vos propres systèmes et avec des URLs de test non-malveillantes — utilisez plutôt les fonctions de test intégrées des solutions de protection email.

FIDO2 est-il vraiment résistant aux attaques quishing AiTM ?

Oui, sous condition. FIDO2 avec des clés matérielles (YubiKey, etc.) ou avec Windows Hello Entreprise est résistant au phishing AiTM car l'authentification est liée à l'origine (URL) du site. Un proxy AiTM a une URL différente de l'URL légitime, donc la validation FIDO2 échoue automatiquement. Microsoft Authenticator avec Number Matching est partiellement résistant — il résiste aux MFA fatigue attacks mais pas à toutes les formes d'AiTM.