

3 menaces à connaître ce mois-ci



Le message du mois

Un mail peut provenir d'un service connu, afficher une page Microsoft authentique ou être rédigé sans faute. Le bon réflexe n'est plus seulement de "repérer un mauvais mail" :
Il faut vérifier l'action demandée et le contexte.

1

Faux remboursement d'impôt : la saison du phishing fiscal

Cybermalveillance.gouv.fr a rappelé en juillet, avec une mise à jour le 3 août 2026, que les périodes de remboursement d'impôt sont exploitées par des campagnes qui imitent l'administration fiscale. Le message annonce un remboursement ou un trop-perçu et renvoie vers un faux site destiné à collecter des informations personnelles ou bancaires.

Pourquoi vous êtes concerné

Un freelance ou un salarié peut être ciblé à titre personnel sur son téléphone, puis réutiliser un mot de passe identique sur un compte professionnel. La frontière perso/pro est souvent le point d'entrée.

Ce qui doit vous alerter

Lien reçu par SMS ou e-mail, montant de remboursement mis en avant, urgence à "confirmer" vos coordonnées, demande de carte bancaire ou d'identifiants. Vérifiez directement depuis le portail officiel saisi manuellement dans le navigateur.



2

Microsoft 365 : le phishing peut contourner une MFA classique

Début août 2026, des chercheurs ont documenté une évolution du service de phishing Greatness visant Microsoft 365. Les attaques peuvent utiliser une technique dite adversary-in-the-middle : la victime se connecte, valide l'authentification, puis l'attaquant récupère la session. Une autre variante détourne des notifications ou des flux légitimes pour rendre le parcours plus crédible.

Le scénario

Vous recevez une notification de messagerie, de visioconférence ou de document partagé. Vous êtes redirigé vers une page de connexion très crédible. Vous saisissez vos identifiants puis validez la MFA. La session obtenue peut ensuite être réutilisée par l'attaquant.

3

Mac : le piège "copier-coller cette commande dans Terminal"

Jamf a publié le 13 août 2026 une analyse d'AmnesiaStealer, un voleur d'informations macOS distribué via de fausses pages GitHub. L'utilisateur est incité à copier une commande dans Terminal. Le malware peut récupérer des données de navigateur, des identifiants, des sessions et certains documents ; un second composant peut permettre le contrôle d'une session Chromium.

Le signal le plus simple

Un site vous demande de copier-coller une commande dans PowerShell, Terminal, Invite de commandes ou Exécuter pour "installer", "vérifier" ou "corriger" quelque chose : arrêtez-vous. C'est une technique de manipulation appelée ClickFix.

Que faire (ou pas!)

- Ne validez jamais une notification MFA que vous n'avez pas déclenchée.
- Accédez aux services Microsoft depuis vos favoris, votre application ou le portail connu plutôt que depuis un lien reçu.
- Pour les administrateurs : privilégier des MFA résistantes au phishing et contrôler les consentements d'applications lorsque l'environnement le permet.

Dans ce cas-là, il faut :

- Installez les logiciels depuis les sources officielles et les magasins approuvés.
- Ne désactivez pas les protections macOS ou Windows pour installer un outil demandé par un site.
- Si vous avez exécuté une commande douteuse, signalez-le immédiatement, même si rien ne semble se passer.

A faire ce mois-ci

Le coin correctifs

Le CERT-FR a publié plusieurs avis et alertes fin juillet et début août 2026, notamment sur Microsoft SharePoint, WordPress, Microsoft Office, navigateurs et composants d'infrastructure. Pour un utilisateur : appliquez les mises à jour de sécurité dès qu'elles sont validées par votre organisation. Pour un freelance chez un client : ne repoussez pas une mise à jour imposée par le client et signalez tout logiciel obsolète nécessaire à la mission.



5 actions simples

- Mettre à jour Windows/macOS, navigateur et applications dès validation par l'organisation.
- Vérifier que la MFA est activée sur la messagerie et les outils cloud principaux.
- Supprimer ou signaler les applications et extensions inutiles ou inconnues.
- Confirmer tout changement de RIB ou paiement inhabituel par un autre canal.
- Signaler un clic ou une commande douteuse immédiatement, sans attendre un symptôme.

Sources et références

- Cybermalveillance.gouv.fr, « Remboursement d'impôt : attention aux tentatives d'hameçonnage », publié le 15/07/2026, mis à jour le 03/08/2026.
- BleepingComputer / recherche ZeroBEC, « Phishing service spoofs RingCentral to steal Microsoft 365 accounts », 04/08/2026.
- Jamf Threat Labs, analyse AmnesiaStealer publiée le 13/08/2026 ; changelog de protection Jamf mis à jour début août.
- CERT-FR / ANSSI, alertes et avis de sécurité publiés fin juillet et début août 2026.
- CNIL, recommandations sur les mots de passe, l'authentification et les violations de données.