

5 minutes pour protéger vos comptes, vos missions et vos paiements.

Le mois d'août rappelle une tendance simple : les attaques efficaces utilisent souvent une information crédible, une urgence plausible et une action demandée à la victime.

À retenir : **phishing** ciblé, faux RIB, faux numéro d'opposition, comptes cloud et ClickFix.



Le message du mois

Une information correcte ne prouve pas que l'interlocuteur est légitime. Avant un paiement, un changement de RIB ou une transmission sensible, vérifiez par un canal indépendant.

Quand la confiance devient le point d'entrée

Données fiscales : le phishing peut devenir beaucoup plus crédible

Des informations exactes ou plausibles peuvent être réutilisées dans de faux emails, SMS ou appels. Le piège ne repose pas forcément sur une faute grossière : il repose sur la crédibilité du contexte.

Signaux : Demande de régularisation, lien vers un faux espace fiscal, RIB ou carte bancaire, ton pressant.

Action à prendre : Ouvrez vous-même le site officiel ou l'application habituelle. Ne partez jamais du lien reçu.

Données fiscales : le phishing peut devenir beaucoup plus crédible

Un SMS signale un paiement suspect et fournit un numéro "service opposition". La victime appelle et se retrouve face à un faux conseiller.

Signaux : Code demandé, validation urgente, interlocuteur qui vous guide dans l'application bancaire.

Action à prendre : N'utilisez que le numéro déjà enregistré dans votre téléphone, votre carte ou l'application bancaire.

Faux RIB / faux dirigeant : la vérification hors email devient la règle

Une boîte mail compromise ou une usurpation d'identité peut suffire à détourner un paiement. Même une adresse habituelle n'est pas une preuve.

Signaux : Nouveau RIB, urgence inhabituelle, demande de confidentialité, changement soudain d'interlocuteur.

Action à prendre : Tout changement d'information clé (RIB, mail, téléphone,...) doit être confirmé par un second canal avec un numéro déjà connu.

La double authentification aide, mais elle ne remplace pas la vigilance

MICROSOFT 365 / GOOGLE WORKSPACE

Un faux document partagé peut mener au vol de compte Vous recevez un lien vers un document, une alerte de sécurité ou une reconnexion. La page imite le service attendu. L'objectif est de récupérer vos identifiants et, dans certains scénarios, votre session après validation.

Signaux : Nom de domaine inhabituel, demande de reconnexion inattendue, invitation "urgente", MFA que vous n'avez pas déclenchée.

Action à prendre : Ouvrez vous-même Microsoft 365, Google, SharePoint ou l'outil cloud depuis vos favoris. Refusez toute MFA non initiée par vous.

Avant de cliquer

Passez la souris sur le lien ou ouvrez l'outil depuis votre favori. Vérifiez le domaine.

Pendant la connexion

Une demande MFA inattendue doit être refusée. Ne validez pas "pour voir".

En cas de doute

Changez le mot de passe, révoquez les sessions si possible et signalez rapidement.

Le piège ClickFix : quand la victime lance elle-même la commande

Faux CAPTCHA, faux téléchargement, vraie commande malveillante

Le site affiche une fausse erreur ou une fausse procédure d'installation puis vous demande d'ouvrir Terminal, PowerShell ou un outil système. Une commande copiée-collée peut alors installer un logiciel voleur de mots de passe ou de sessions.

Signaux : "Ouvrez Terminal", commande curl/bash, logiciel trouvé via publicité, domaine ressemblant à GitHub, autorisation système incohérente.

Action à prendre : Un CAPTCHA n'a aucune raison de demander Terminal ou PowerShell. Téléchargez depuis l'éditeur ou un magasin officiel et comprenez toute commande avant exécution.

Postes

Windows / macOS : appliquez les mises à jour de sécurité et redémarrez les postes si nécessaire.

Navigation

Chrome / Firefox / Edge : le navigateur reste une surface d'attaque majeure. Gardez-le à jour.

Outils tech

VPN, GitLab, Docker, plugins, packages et dépendances : suivez aussi les correctifs côté consultant technique.

A faire ce mois-ci



Actions simples

1. **Sécuriser les connexions** : MFA active sur la messagerie et les outils cloud. Toute MFA inattendue doit être refusée.
2. **Mettre à jour** : Ordinateur, navigateur, smartphone et applications. Les profils techniques ajoutent leurs composants exposés.
3. **Verrouiller les paiements** : Aucun changement de RIB ou de compte de versement sur la seule base d'un email.
4. **Séparer les usages** : Évitez les mots de passe réutilisés et les comptes personnels pour les données client.
5. **Signaler vite** : Après un clic, un code transmis ou une MFA validée par erreur : changez le mot de passe et prévenez sans attendre.



Mini Quiz

Affirmation	Verdict
Un email envoyé depuis l'adresse habituelle d'un fournisseur suffit pour valider un nouveau RIB.	FAUX
Je refuse une MFA que je n'ai pas moi-même déclenchée.	VRAI
Un CAPTCHA peut légitimement me demander d'ouvrir Terminal ou PowerShell.	FAUX
Pour appeler ma banque après un SMS suspect, j'utilise le numéro indiqué dans le SMS.	FAUX
Un fraudeur peut connaître des informations exactes sans être l'administration ou le fournisseur.	VRAI

Sources et références

- ANSSI / CERT-FR
- Cybermalveillance.gouv.fr
- CNIL
- CISA
- Microsoft Security
- Google Security / Google Cloud