FICHE RÉFLEXE CYBERSÉCURITÉ

PHISHING / HAMEÇONNAGE

ALERTE UTILISATEUR

J'ai reçu un email suspect / J'ai cliqué sur un lien — Que faire ?

SECTION 1 — COMMENT RECONNAÎTRE UN EMAIL DE PHISHING

5 INDICES VISUELS **Inspectez chaque email suspect avec ces critères**

🔗 **Lien suspect au survol**

Passez votre souris sur le lien sans cliquer. L'URL affichée ne correspond pas au site supposé de l'expéditeur.

✍️ **Fautes d'orthographe / mise en forme**

Logos pixelisés, caractères accentués mal encodés, formules maladroites — signe d'un message généré en masse.

🔌 **Adres expéd doute**

Le nor connu l'adres contie caract un dor inconn faute : « serv securit

🔐 Dema d'info sensi

Aucun organi sérieu (banqu impôts Ameli) demar identifi numér ou mo passe

SECTION 2 — J'AI CLIQUÉ — LES 5 PREMIÈRES MINUTES

URGENCE **Agissez dans cet ordre précis**

Min 1 **Ne pas fermer le navigateur**

Notez l'URL complète de la page frauduleuse (screenshot), puis fermez l'onglet.

Min 2 **Changer immédiatement votre mot de passe**

Sur le vrai site de l'organisme concerné, depuis un autre appareil si possible. Activez la double authentification (2FA).

Min 3 **Scanner votre poste**

Lancez une analyse antivirus complète. Si vous avez téléchargé un fichier, ne l'ouvrez pas et signalez-le à votre service informatique.

Min 4 **Alerter votre responsable / service informatique**

Par téléphone, pas par email. Décrivez ce qui s'est passé, l'URL, ce que vous avez saisi.

Min 5 **Signaler l'email**

Transférez l'email à signal-spam.fr et signalez le lien sur phishing-initiative.fr. Ne supprimez pas l'email avant signalement.

SECTION 3 — OÙ SIGNALER

SIGNALEMENT **Deux plateformes officielles gratuites**

signal-spam.fr

Signalement des emails frauduleux — transférez directement depuis votre messagerie

phishing-initiative.fr

Signalement des URLs frauduleuses — permet le blocage rapide du site dans les navigateurs

Besoin d'un accompagnement ou d'une sensibilisation de vos équipes ?

ayinedjimi-consultants.fr/contact