FICHE PRATIQUE

Reconnaître un email de phishing

Le phishing reste la porte d'entrée n°1 des cyberattaques contre les TPE/PME.

Les 5 signaux rouges

- **Urgence** : « Votre compte sera bloqué sous 24 h ».
- **Émetteur étrange** : un email qui prétend venir de votre banque mais finit par @gmail.com.
- **Lien suspect** : survolez-le, l'URL réelle s'affiche en bas du navigateur.
- **Pièce jointe inattendue** : facture, CV, ZIP… surtout d'un inconnu.
- **Demande inhabituelle** : virement « urgent » du dirigeant, changement d'IBAN fournisseur.

Le réflexe en 3 temps

- **Stop** : ne cliquez sur rien, ne répondez pas.
- **Vérifiez** par un autre canal : appelez votre interlocuteur sur son numéro habituel.
- **Signalez** à **signal-spam.fr** ou **phishing-initiative.fr**, puis supprimez.

Les arnaques du moment

- Faux mail Ameli, Impôts, Chronopost, Vinted, Netflix.
- Fausse alerte « connexion suspecte Microsoft 365 ».
- Fraude au président : usurpation du dirigeant pour déclencher un virement.

Côté entreprise

- Activez la **double authentification** sur tous les comptes pro.
- Mettez en place **SPF, DKIM, DMARC** sur votre nom de domaine.
- Formez vos équipes au moins **1 fois par an** avec des cas concrets.

Tester vos équipes ?
BigFamily organise des simulations de phishing pédagogiques, sans piège ni honte.