**Comment réagir à une attaque de phishing dans une petite entreprise – en moins de 30 minutes**

**Par Stella Barbarella | Spécialiste en cybersécurité**

**Dédicace**

"À ceux qui savent qu'ils sont plus intelligents que la machine – et plus audacieux que leurs propres doutes."  
— Stella Barbarella, Série CyberNerve

**1. Détecter la menace – S'agit-il d'un incident de phishing ?**

Une attaque de phishing commence souvent par un simple clic maladroit. Posez-vous les questions suivantes :

* Quelqu'un a-t-il reçu un e-mail inhabituel ?
* Ont-ils cliqué sur un lien, téléchargé une pièce jointe, ou saisi des identifiants ?
* Des informations sensibles ont-elles été transmises ?

**Si oui — activez immédiatement le mode réponse à incident.**

**2. Les 30 premières minutes – Actions d'urgence**

**a) Isolez l'appareil :** Débranchez le câble Ethernet ou désactivez le Wi-Fi.  
**b) Prévenez l'équipe IT ou le support technique interne** (calmement – évitez la panique générale).  
**c) Demandez précisément : Que s'est-il passé ?**

* Qui a reçu l’e-mail de phishing ?
* Y a-t-il eu une interaction (clic, téléchargement, réponse) ?
* Quelles informations ont été compromises (identifiants, documents, données financières) ?

**d) Changez immédiatement les mots de passe** (e-mail, VPN, outils SaaS).  
**e) Vérifiez les règles de messagerie** (par exemple, transferts automatiques suspects).

**3. Contention et évaluation de l'impact**

* Analysez les appareils affectés avec un antivirus ou EDR.
* Cherchez des e-mails similaires dans les autres boîtes aux lettres.
* Informez les utilisateurs concernés **sans transférer l'e-mail malveillant**.
* Documentez les éléments essentiels :
  + Chronologie de l'incident
  + Impact estimé
  + Utilisateurs touchés
  + Systèmes concernés

**Pourquoi ?** Une bonne documentation est indispensable pour des raisons juridiques, assurantielles et d'apprentissage.

**4. Communication et signalement**

* Alertez la direction et le DPO (si applicable).
* Si des données personnelles ont été exposées, préparez une notification réglementaire (ex: RGPD).
* Maintenez une communication calme et pédagogique — **sans chercher de coupable.**
* Soutenez l’utilisateur impacté — il est victime, non responsable.

**5. Prévention : Construire une entreprise résistante au phishing**

* Organisez des formations de sensibilisation courtes, régulières et pratiques.
* Activez l’authentification à deux facteurs (2FA) sur tous les accès critiques.
* Configurez les protocoles SPF, DKIM et DMARC sur vos domaines e-mail.
* Déployez des outils EDR de base (même gratuits).
* Mettez en place une **Check-list de réponse au phishing** accessible à tous.
* Favorisez une culture de **déclaration rapide des incidents**.

**6. Les nouvelles menaces de phishing (Tendances 2025)**

Le phishing moderne est plus sophistiqué :

* **E-mails générés par IA :** Hautement personnalisés, difficiles à détecter.
* **Phishing vocal (vishing) avec deepfake :** Imitations d'appels de cadres.
* **Réutilisation de données issues de fuites :** Attaques basées sur LinkedIn, fuites de bases de données.
* **Business Email Compromise (BEC) :** Exploitation de la confiance sans malware.

En 2025, les attaques de phishing ciblent l'humain, pas les systèmes.  
**Votre meilleur pare-feu est l’intelligence humaine.**

**7. Ressources et outils recommandés (par Stella)**

**Simulateurs de phishing :**

* Gophish (gratuit et open-source)
* KnowBe4 (version gratuite)
* Phishing Tackle

**Outils d'analyse :**

* VirusTotal (analyse de fichiers/liens)
* MXToolbox (vérification de domaines e-mail)
* URLScan.io (analyse d'URL suspectes)
* EmailHeaders.net (analyse d'en-têtes e-mails)

**Sources de veille cybersécurité :**

* ENISA Threat Landscape (EU)
* Alertes CISA (US)
* CERT-FR (France)
* ANSSI Rapports

**8. Check-list imprimable : Réponse à un incident de phishing**

**Par Stella Barbarella | Série CyberNerve**

**Identifier et isoler l'incident**

**Analyser et documenter**

**Contenir l'impact**

**Informer et communiquer**

**Nettoyer et restaurer**

**Apprendre et prévenir**

**✉ À imprimer et garder à portée de main pour toute PME ou indépendant !**

**© Stella Barbarella — CyberNerve Series**