FICHE RÉFLEXE CYBERSÉCURITÉ

J'AI CLIQUÉ SUR UN LIEN SUSPECT

URGENCE UTILISATEUR

Les 5 premières minutes — Suivez l'arbre de décision selon ce qui s'est passé

Restez calme. Ne fermez rien encore. Lisez d'abord les questions ci-dessous et identifiez votre situation.

🔐 Question 1 — Avez-vous saisi des identifiants ou un mot de passe sur la page ?

OUI — **Changement de mot de passe immédiat — priorité absolue**

1. **Rendez-vous sur le VRAI site** de l'organisme concerné (tapez l'URL à la main)
2. **Changez votre mot de passe immédiatement** depuis un autre appareil si possible
3. **Activez la double authentification (2FA)** si ce n'est pas déjà fait
4. **Changez le même mot de passe** sur tous les autres sites où vous l'utilisez
5. Signalez à votre responsable ou service informatique

NON — **Pas d'identifiants saisis — passez à la question 2**

1. La page s'est simplement ouverte — risque limité mais pas nul
2. Fermez l'onglet, notez l'URL pour la signaler

📄 Question 2 — Avez-vous téléchargé ou ouvert un fichier depuis ce lien ?

OUI — **Isolez le poste — risque d'infection**

1. **Déconnectez immédiatement** le câble réseau / désactivez le Wi-Fi
2. **N'ouvrez pas le fichier** si ce n'est pas encore fait — surtout si .exe, .zip, .doc avec macros
3. **Appelez votre service informatique** par téléphone — ne pas utiliser le poste
4. Ne rallumez pas / ne redémarrez pas le poste sans instruction de l'IT

NON — **Aucun fichier téléchargé — passez à la question 3**

1. Risque réduit — mais vérifiez quand même le dossier Téléchargements

💳 Question 3 — Avez-vous saisi des données bancaires ou personnelles (CB, IBAN, N° sécu) ?

OUI — **Opposition bancaire immédiate**

1. **Appelez immédiatement votre banque** au numéro au dos de votre carte pour faire opposition
2. **Signalez sur cybermalveillance.gouv.fr** et déposez plainte
3. Pour le N° de sécu : signalez à l'Assurance Maladie — risque d'usurpation d'identité
4. Surveillez vos relevés de compte dans les semaines suivantes

NON — **Pas de donnée bancaire saisie**

1. Lancez une analyse antivirus complète de votre poste
2. Signalez le lien frauduleux sur phishing-initiative.fr

DANS TOUS LES CAS — ACTIONS SYSTÉMATIQUES

- ✓ Faites une capture d'écran de la page suspecte (URL visible) avant de fermer
- ✓ Signalez le lien sur phishing-initiative.fr pour protéger les autres utilisateurs
- ✓ Prévenez votre service informatique ou responsable, même si tout semble normal
- ✓ Lancez une analyse antivirus complète de votre poste dans les 24h

Besoin d'une réponse à incident ou d'une sensibilisation de vos collaborateurs ?

ayinedjimi-consultants.fr/contact