Cybersécurité : Les bons réflexes au quotidien

Sensibilisation pour tous les collaborateurs

Pourquoi la cybersécurité nous concerne tous ?

1 entreprise sur 2 touchée

D'ici 2025, une entreprise sur deux sera victime d'une cyberattaque. Personne n'est à l'abri.

Coût moyen 184 000 €

Le coût moyen d'une cyberattaque pour une PME peut atteindre 184 000 €. Cela impacte directement notre activité.

Les hackers vous ciblent en premier

Les serveurs sont souvent bien protégés. Les hackers préfèrent cibler les employés pour s'introduire dans nos systèmes.

Message clé : Vous êtes la première ligne de défense contre les cybermenaces. Votre vigilance est essentielle.

Le Phishing (hameçonnage)

Le phishing est une technique de fraude en ligne qui consiste à se faire passer pour un organisme légitime (banque, administration, fournisseur, etc.) afin de soutirer des informations confidentielles.

Comment le reconnaître ?

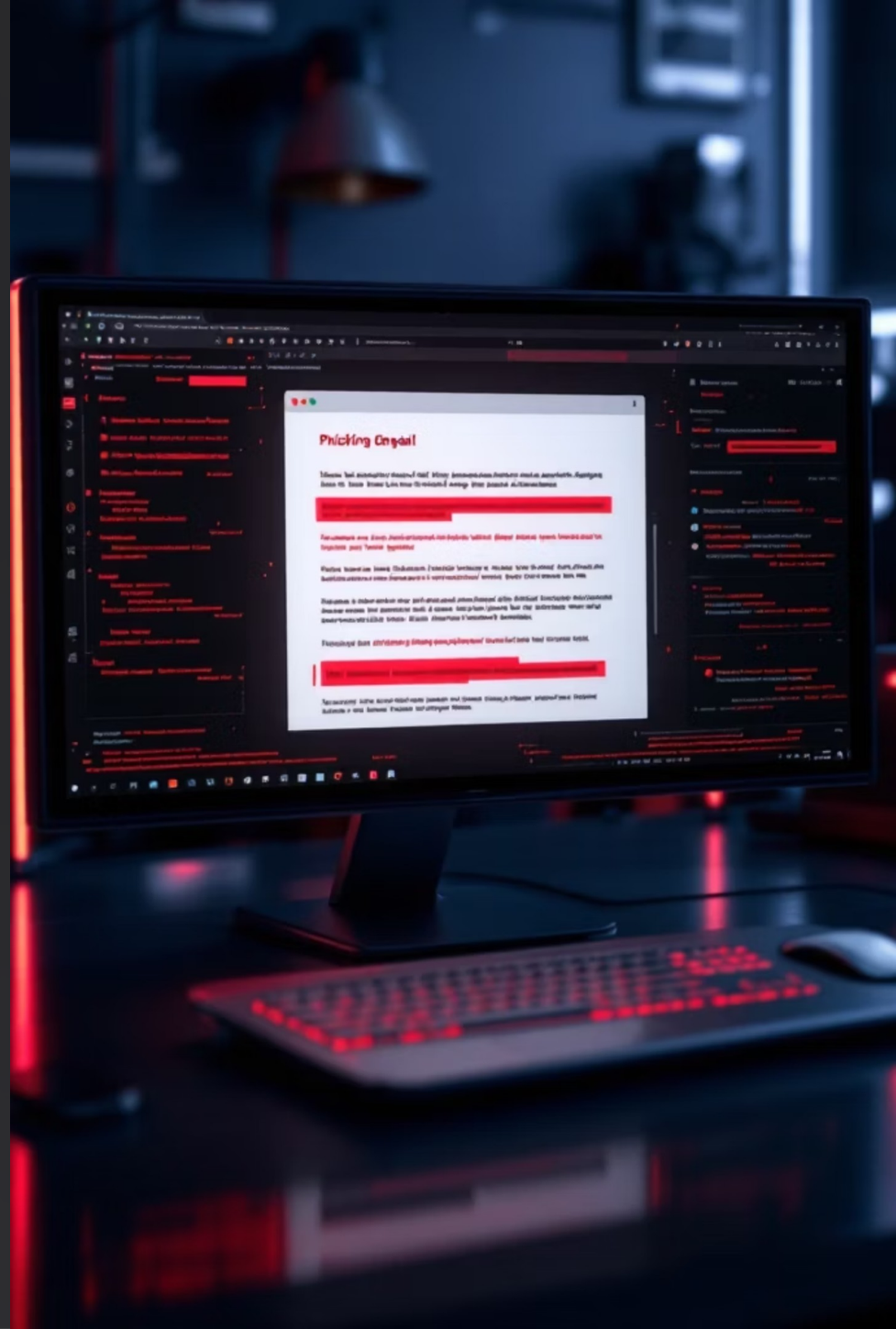
- Expéditeur suspect ou inconnu.
- Fautes d'orthographe ou de grammaire.
- Lien bizarre (URL incohérente).
- Sentiment d'urgence ou menace.
- Demande d'informations confidentielles.

Que faire ?

- NE CLIQUEZ PAS sur les liens ou les pièces jointes.
- SIGNEZ l'email au service IT.
- SUPPRIMEZ le message suspect.

Conséquences

Vol de vos données, accès à nos systèmes, usurpation d'identité. Protégeons nos informations et l'entreprise !



Les Ransomwares (rançongiciels)

Un ransomware est un logiciel malveillant qui chiffre vos fichiers et bloque l'accès à votre système, exigeant une rançon pour les débloquer.

Comment ça arrive ?

- Pièce jointe infectée dans un email.
- Lien malveillant sur un site web.
- Clé USB inconnue et infectée.

Conséquences

Arrêt total de l'activité, perte irréversible de données, paiement de rançons pouvant se chiffrer en milliers d'euros.

Exemple concret :

En 2022, l'hôpital de Corbeil-Essonnes a été victime d'un ransomware, entraînant des perturbations majeures dans les soins et un coût financier important.

Que faire immédiatement ?

Déconnectez votre poste du réseau (WiFi/câble) et **alertez sans délai le service IT.**

Les mots de passe

Vos mots de passe sont les clés de vos accès. Ils doivent être uniques et difficiles à deviner.

Règles d'or

- Minimum 12 caractères.
- Mélange de majuscules, minuscules, chiffres et symboles.
- Un mot de passe différent par service.
- Activez la double authentification (MFA) si disponible.

À ne jamais faire

- Écrire son mot de passe sur un post-it.
- Le partager, même avec un collègue.
- Utiliser le même mot de passe partout.

Le poste de travail

Votre ordinateur contient des informations précieuses. Protégez-le physiquement.

Verrouillez l'écran

Dès que vous quittez votre bureau, même pour quelques minutes, appuyez sur **Windows + L** (ou Cmd + Ctrl + Q sur Mac).

Ne pas laisser allumé

Ne laissez jamais votre ordinateur allumé et déverrouillé sans surveillance. Éteignez-le en fin de journée.

Clés USB inconnues

N'insérez jamais une clé USB que vous ne connaissez pas ou que vous avez trouvée. Elle pourrait être infectée.

Logiciels non autorisés

N'installez aucun logiciel sans l'approbation du service IT pour éviter les vulnérabilités.

Emails et navigation

Soyez vigilant avec ce que vous recevez et où vous naviguez sur internet.

- **Pièces jointes douteuses :** Ne les ouvrez jamais si l'expéditeur est inconnu ou le contenu suspect.
- **Vérifier les URLs :** Survolez les liens avec votre souris avant de cliquer pour voir la vraie adresse.
- **WiFi public :** Évitez d'utiliser les réseaux WiFi publics non sécurisés pour des activités professionnelles sans VPN.
- **Messagerie pro :** N'utilisez pas votre email professionnel pour vos usages personnels. Cela réduit les risques de contamination.
- **Téléchargements :** Ne téléchargez jamais de logiciels ou de fichiers depuis des sites non officiels.

Les données sensibles

La protection des données est une responsabilité partagée. Le non-respect peut entraîner de lourdes sanctions.

- **Supports personnels :** Ne stockez jamais de données clients ou confidentielles de l'entreprise sur vos clés USB personnelles, clouds privés ou disques durs externes.
- **Email non chiffré :** N'envoyez jamais de données confidentielles ou personnelles par email sans chiffrement adéquat.
- **Politique de classification :** Respectez scrupuleusement la politique de classification des données de l'entreprise pour gérer les informations selon leur niveau de sensibilité.
- **RGPD :** Le Règlement Général sur la Protection des Données protège les informations personnelles. Toute fuite peut entraîner de très lourdes amendes et nuire gravement à la réputation de l'entreprise.

En cas d'incident : que faire ?

Ne pas paniquer

Déconnecter réseau

Contacter IT

Ne pas résoudre seul

La rapidité de réaction est cruciale pour limiter les dégâts d'une cyberattaque. Suivez ces étapes.

Checklist des bons réflexes au quotidien

Ces gestes simples protègent vos données et celles de l'entreprise.

- [ ] **Je verrouille mon écran quand je pars**
- [ ] **Je vérifie l'expéditeur avant d'ouvrir un email**
- [ ] **Je signale tout comportement suspect au service IT**
- [ ] **Je n'utilise pas de clé USB inconnue**
- [ ] **Je me déconnecte en fin de journée**
- [ ] **Je ne clique pas sur des liens douteux**
- [ ] **Je ne partage pas mon mot de passe**