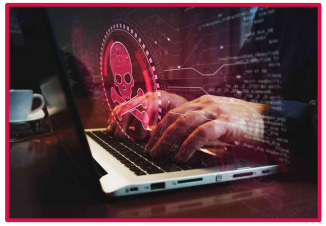
BONNES PRATIQUES

- **Sécuriser** le système informatique, le réseau (+ *site internet*), les postes de travail
  - ☛ *Politique de mots de passe rigoureuse, accès aux données, antivirus, pare-feu, ...*
- Faire appel à des **prestataires de confiance**
- **Sensibiliser** l'ensemble des agents au risque cyber
- Séparer ses usages **pro** / **perso** (*réseaux sociaux*)
- Réaliser et gérer les **sauvegardes**
- Effectuer les **mises à jour** régulièrement
- Protéger également les **appareils mobiles**
- **Anticiper** le risque de perte ou de divulgation des données **...**

CYBER SÉCURITÉ

Gendarmerie des VOSGES

EN CAS D'ATTAQUE ?



LES ÉTAPES CLÉS

1 PREMIERS RÉFLEXES

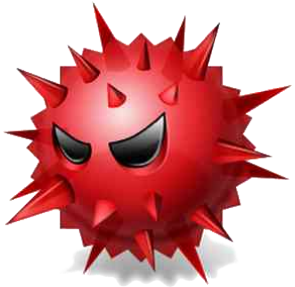
- ALERTEZ IMMÉDIATEMENT VOTRE SUPPORT INFORMATIQUE
- ISOLEZ LES SYSTÈMES ATTAQUÉS
- CONSTITUEZ UNE ÉQUIPE DE GESTION DE CRISE
- TENEZ UN REGISTRE DES ÉVÉNEMENTS
- PRÉSERVEZ LES PREUVES DE L'ATTAQUE

2 PILOTER LA CRISE

- METTEZ EN PLACE DES SOLUTIONS DE SECOURS
- DÉCLAREZ LE SINISTRE AUPRÈS DE VOTRE ASSUREUR
- ALERTEZ VOTRE BANQUE
- DÉPOSEZ PLAINTE
- IDENTIFIEZ L'ORIGINE DE L'ATTAQUE ET SON ÉTENDUE
- NOTIFIEZ L'INCIDENT À LA CNIL
- GÉREZ VOTRE COMMUNICATION

3 SORTIR DE LA CRISE

- TIREZ LES ENSEIGNEMENTS DE L'ATTAQUE ET DÉFINISSEZ LES PLANS D'ACTION
- FAITES UNE REMISE EN SERVICE PROGRESSIVE ET CONTRÔLÉE



CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

ComCyberGend