

Procédure En Cas De Cyberattaques

Objectif :

Mettre en place un protocole efficace pour contenir et neutraliser toute menace cyber sur les infrastructures systèmes et réseaux.

Matériel nécessaire :

- Un ordinateur (portable ou unité centrale)
- Un téléphone (Portable ou fixe)

Attention !

Cette documentation technique n'est pas un guide de mesures préventives. Elle est adressée à tout utilisateur étant victime de l'une de ces attaques informatiques :

- Phishing
- Ransomware
- Escroquerie au faux support informatique

Version 1.1

Mise à jour le : 25/06/2025

Rédacteur : Axel ROUX & Sébastien SIMON

Vérificateur : Emmanuel BROCHARD

Table des matières

1/ L'attaque par Phishing :	3
Identifier l'attaque	3
Contenir le risque immédiatement	4
Analyser et collecter les preuves.....	4
Signaler l'attaque :	4
Renforcer ta sécurité	4
2/ L'attaque par Ransomware :	5
Analyser l'attaque	5
Isoler immédiatement les systèmes infectés	5
Alerter les bonnes personnes.....	5
Ne jamais payer la rançon.....	6
Restaurer les données.....	6
Déclarer l'incident.....	6
Renforcer la sécurité	6
3/ Attaque au faux support informatique.....	6
Ne jamais appeler ou cliquer.....	6
Fermer la page ou redémarrer	7
Changer les mots de passe	7
Conserver les preuves	7
Signaler l'arnaque	7
Faire un scan complet	7
4/ Fiche réflexe	8
10 gestes essentiels à adopter.....	8

1/ L'attaque par Phishing :

L'hameçonnage ou phishing est une forme d'escroquerie sur internet.

Le fraudeur se fait passer pour un organisme que vous connaissez (banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme. Il vous envoie un mail vous demandant généralement de "mettre à jour" ou de "confirmer vos informations suite à un incident technique", notamment vos coordonnées bancaires (numéro de compte, codes personnels, etc.).

Identifier l'attaque


Exemple :

De Votre Conseiller <oteck@schulte-goecking.de>  
Pour oteck@schulte-goecking.de <oteck@schulte-goecking.de> 
Sujet SG - Rappel 02:12




Bonjour, 

Dans le cadre de la nouvelle réglementation en matière de sécurité, nous vous informons qu'il est désormais nécessaire de mettre à jour la liste des bénéficiaires tous les 6 mois. Nous avons constaté qu'une modification récente des coordonnées d'un de vos bénéficiaires nécessite une mise à jour.

Pour éviter toute interruption de votre accès à l'option de virement en ligne, nous vous invitons à procéder à cette mise à jour dès que possible. 

Merci de cliquer sur le lien ci-dessous pour effectuer cette action :

Mettre à jour mes bénéficiaires 

Sans cette action, l'accès à l'option de virement en ligne sera temporairement bloqué.

Merci de votre compréhension.

Cordialement,

Société Générale

  <https://webcontactactuspa.page.link/YUEHZKHUH0001>

- Vérifier si un lien frauduleux a été cliqué ou si vous avez saisis vos identifiants.
- Regarder si l'email, le SMS ou le site frauduleux est encore accessible pour l'analyse.
- Ne cliquez sur rien de plus !

Version 1.1

Mise à jour le : 25/06/2025

Rédacteur : Axel ROUX & Sébastien SIMON

Vérificateur : Emmanuel BROCHARD

Contenir le risque immédiatement

- Changer les mots de passe des comptes compromis ou suspects (email, réseau pro, services en ligne).
- Activer l'authentification à deux facteurs (A2F) si ce n'est pas déjà fait.
- Déconnecter les sessions actives sur internet (Google, Microsoft Outlook, réseaux sociaux...).
- Prévenir son équipe informatique.

Analyser et collecter les preuves

- Garder une copie du mail ou du SMS suspect.
- Noter la date, l'heure, l'expéditeur, et les URL utilisées.
- Vérifier les journaux d'accès (tentatives de connexion inhabituelles).

Signaler l'attaque :

- En fonction du pays :

Pays	Plateforme de signalement officielle
FR France	cybermalveillance.gouv.fr ou Signal Spam
EU Union Européenne	econsumer.gov (plateforme internationale)
us États-Unis	FTC Complaint Assistant ou IC3
CA Canada	Centre antifraude du Canada
GB Royaume-Uni	Action Fraud
DE Allemagne	BSI – Bundesamt für Sicherheit in der Informationstechnik
 International	Phishing Initiative (pour signaler un site frauduleux)

- Alertez vos contacts si vous pensez qu'un email est parti depuis votre adresse.
- Si des informations bancaires ont été données, contactez votre banque immédiatement.

Renforcer ta sécurité

- Analyser votre ordinateur avec un antivirus ou un outil anti-malware (Windows Defender).
- Vérifier les règles de transfert ou les redirections mail (certaines attaques les modifient).
- Mettre à jour les logiciels (système, navigateur, extensions...).

2/ L'attaque par Ransomware :

Le rançongiciel ou ransomware est un type d'attaque informatique qui bloque l'accès à l'appareil ou aux fichiers d'une victime et qui exige le paiement d'une rançon en échange du rétablissement de l'accès.

Analyser l'attaque

Exemple :



- ☐ Identifier le type de ransomware (nom, extension des fichiers, message affiché).

Isoler immédiatement les systèmes infectés

- Débrancher les machines touchées du réseau (Wi-Fi, Ethernet, VPN).
- Couper l'accès à Internet pour éviter la propagation.
- Ne redémarrer pas les systèmes sans analyse préalable.

Alerter les bonnes personnes

- Prévenir votre équipe IT ou votre prestataire cybersécurité.
- Si vous êtes en entreprise, activer le plan de gestion de crise.
- En France, vous pouvez aussi contacter cybermalveillance.gouv.fr pour de l'assistance.

Version 1.1

Mise à jour le : 25/06/2025

Rédacteur : Axel ROUX & Sébastien SIMON

Vérificateur : Emmanuel BROCHARD

Ne jamais payer la rançon

- Payer ne garantit ni la récupération des données, ni la fin de l'attaque. □
Cela encourage les cybercriminels à recommencer.

Restaurer les données

- Utiliser des sauvegardes saines et non connectées au moment de l'attaque.

Déclarer l'incident

- Déposer plainte auprès des autorités (police, gendarmerie).
- Si des données personnelles sont concernées, notifier la CNIL dans les 72h.

Renforcer la sécurité

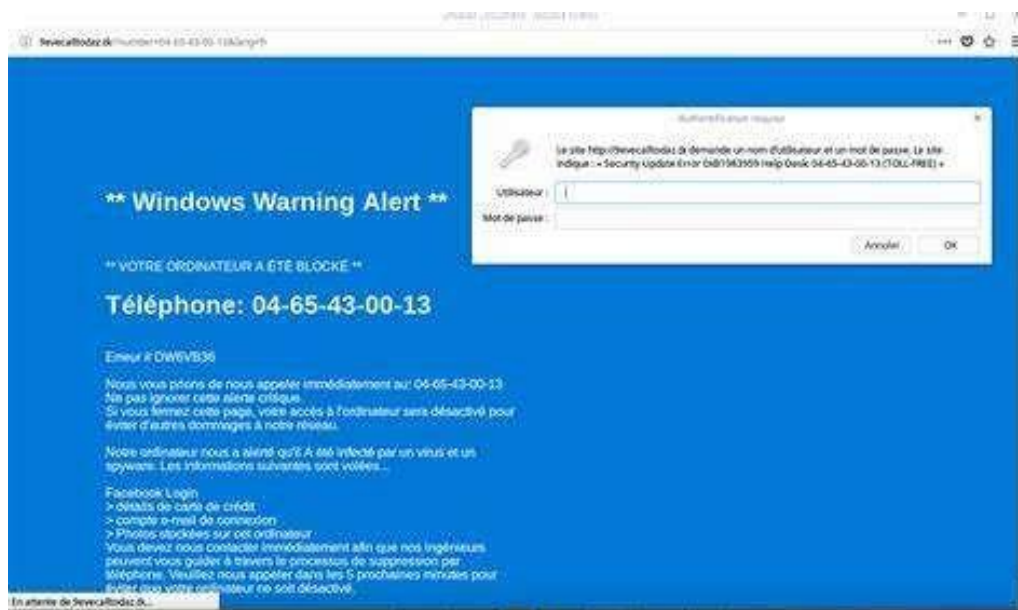
- Mettre à jour tous les systèmes et logiciels.
- Activer l'authentification à deux facteurs (2FA).
- Sensibiliser les utilisateurs aux risques (phishing, pièces jointes, etc.).

3/ Attaque au faux support informatique

Une attaque au faux support informatique (ou arnaque au faux support technique) est une escroquerie où un cybercriminel se fait passer pour un technicien (souvent Microsoft, Apple, etc.) pour t'effrayer et te pousser à lui donner l'accès à ton ordinateur ou à payer un faux dépannage. Voici comment réagir efficacement :

Ne jamais appeler ou cliquer

Exemple :



Version 1.1

Mise à jour le : 25/06/2025

Rédacteur : Axel ROUX & Sébastien SIMON

Vérificateur : Emmanuel BROCHARD

- Ignorer les messages d’alerte qui apparaissent soudainement (souvent en plein écran, avec des sons ou des comptes à rebours).
- Ne composer jamais le numéro affiché.
- Ne cliquer sur aucun lien ou bouton.

Fermer la page ou redémarrer

- Fermer l’onglet ou le navigateur via le gestionnaire de tâches (Ctrl+Shift+Esc sur Windows).
- Si bloqué, redémarrer l’ordinateur en mode sans échec.

Changer les mots de passe

- Si vous avez donné un accès à distance ou saisi des identifiants, change immédiatement tes mots de passe (email, comptes bancaires, etc.).
- Activer l’authentification à deux facteurs (A2F) si possible.

Conserver les preuves

- Faire une capture d’écran du message frauduleux.
- Noter l’URL, le numéro de téléphone affiché, l’heure et la date.
- Ne supprimer rien avant d’avoir tout sauvegardé pour une éventuelle plainte.

Signaler l’arnaque

- En France, vous pouvez signaler l’attaque sur cybermalveillance.gouv.fr ou phishinginitiative.fr.
- Déposer plainte auprès de la police ou de la gendarmerie si tu as subi un préjudice.

Faire un scan complet

- Lancer une analyse antivirus/malware complète (Windows Defender).
- Vérifier les logiciels installés récemment (les arnaqueurs peuvent vous avoir fait installer un outil espion).

4/ Fiche réflexe

10 gestes essentiels à adopter

- Ne jamais cliquer sur un lien suspect
→ Vérifiez l'adresse complète, même si l'expéditeur semble connu.
- Utiliser des mots de passe complexes et uniques
→ Activez l'authentification à deux facteurs (2FA) dès que possible.
- Garder ses logiciels à jour
→ Système d'exploitation, antivirus, navigateur, applications...
- Faire des sauvegardes régulières
→ Stockées dans un espace hors ligne ou dans le cloud sécurisé.
- Vérifier l'identité avant de partager des infos sensibles → En cas de doute, appelez directement la personne concernée.
- Ne jamais installer de logiciel inconnu
→ Téléchargez uniquement depuis les sources officielles.
- Verrouiller son poste lors d'une absence
→ Même pour quelques minutes : `Windows+L`
- Ne pas se connecter à des Wi-Fi publics sans VPN → Les connexions ouvertes sont souvent vulnérables.
- Éviter l'usage personnel sur les postes professionnels → Et inversement : séparation claire des usages.
- Sensibiliser les autres
→ Parlez sécurité autour de vous : famille, collègues, amis.

ASTUCE BONUS :

Utilisez un gestionnaire de mots de passe pour renforcer votre sécurité sans effort.