POLICE

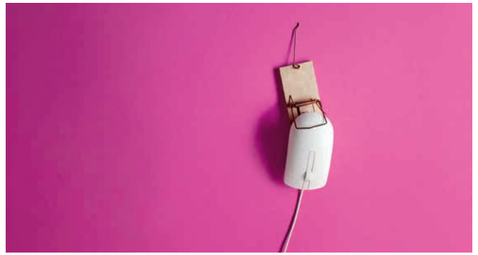
# Cyberattaque – Et maintenant?

## Recommandations pour les personnes touchées

Agir rapidement est décisif lorsque vous êtes victime d'une cyberattaque ou que vous pensez l'être. Les recommandations suivantes vous aideront à maîtriser l'attaque, à limiter les dommages et à protéger votre entourage.

## Prenez des mesures d'urgence

> Pensez-vous qu'un appareil est infecté par un maliciel? Déconnectez l'appareil d'Internet et consultez un spécialiste.
> Avez-vous transmis des mots de passe? Changez-les immédiatement.
> Avez-vous transmis des données de cartes de crédit ou bancaires, ou avez-vous viré de l'argent? Bloquez votre carte et informez-en aussitôt votre banque.
> Vos documents officiels sont-ils passés entre de mauvaises mains? Annulez-les auprès du centre cantonal compétent ou de la police.
> Informez vos connaissances des activités criminelles commises en votre nom.



## Annoncez-vous!

**En cas de dommages: déposez plainte auprès de la police.**
En cas d'infraction, comme le piratage, l'escroquerie ou le chantage, appelez immédiatement la police. Surtout lorsque vous avez effectué un virement ou que vous constatez une fuite de données personnelles.

> En cas d'urgence, appelez le numéro 112
> Déposez plainte. Fixez un rendez-vous dans un poste de police.
> Préparez vos moyens de preuve, tels les messages, les données de contact des auteurs, les extraits bancaires et les appareils concernés.
> Ne réinitialisez les appareils si possible qu'après la mise en sûreté des traces par la police.

Après le dépôt de plainte et l'administration des preuves, la police lance des investigations dont l'objectif est de vérifier d'éventuels liens avec d'autres affaires et de confondre les coupables. La procédure est dirigée par le ministère public compétent.

**Aucun dommage: annonce au Centre national pour la cybersécurité.**
Chaque annonce contribue à identifier au plus tôt des activités criminelles et d'y réagir. Annoncez aussi les cyberattaques avortées ou les tentatives d'escroquerie sans dommage auprès du:

Centre national pour la cybersécurité,
www.report.ncsc.admin.ch

## Faites attention aux attaques suivantes

Restez attentifs même après une cyberattaque. Les criminels peuvent relancer une tentative d'escroquerie avec les données déjà recueillies ou à nouveau réussir à accéder à votre appareil.

**Police cantonale bernoise**
Waisenhausplatz 32
3011 Berne

police.be.ch/cyber

POLICE

# Mobilité en toute sécurité – Même sur Internet

## Recommandations pour les particuliers

Pour se protéger des cyberattaques, il faut combiner des mesures techniques et un bon comportement. Les recommandations suivantes vous aideront à relever votre niveau de sécurité dans le monde numérique.

## Ne vous laissez pas berner

Les criminels dissimulent leur identité en se faisant passer pour des personnes dignes de confiance. Rendez-leur la tâche difficile:

> Ne divulguez aucune information ou donnée confidentielle, comme les mots de passe, les codes de cartes-cadeaux, les informations de cartes de crédit, les documents officiels et des photographies intimes.
> Ne remettez pas d'argent ou d'objets précieux à des personnes que vous ne connaissez pas.
> N'accordez à personne l'accès à votre compte e-banking ou à votre ordinateur.
> Soyez sceptiques envers les promesses généreuses de gains ou les occasions en or.
> Soyez méfiants lorsque l'«Amour de votre vie» ou une soi-disant connaissance vous demande une aide financière sur le net.
> Soyez parcimonieux quant à la publication de renseignements à votre sujet sur Internet, dans les réseaux sociaux ou les tchats. Les criminels les collectent pour préparer leur attaque.
> Ne cliquez pas sur des liens suspects. Ne téléchargez pas de données ou de programmes qui vous paraissent étranges.

## Protégez vos systèmes et vos données

Les criminels abusent des failles techniques, pour pénétrer dans les systèmes et se saisir des données. Rendez-leur l'accès difficile:

> Utilisez des mots de passe sûrs. Un mot de passe sûr:
  > est généré selon le principe du hasard et contient au moins 12 caractères.
  > contient des majuscules et minuscules, des chiffres et des caractères spéciaux.
  > n'est utilisé que pour une seule application. Un gestionnaire de mots de passe vous aidera à gérer vos différents mots de passe.
  > est complété par une authentification à deux facteurs.
> Utilisez des appareils avec des fonctions de sécurité. Activez un pare-feu, une protection contre les virus et les menaces, une mise à jour automatique et un filtre Internet.
> Désactivez les macros dans les applications Office. Ce sont des portes d'entrée potentielles pour les maliciels.
> Séparez votre accès Internet entre réseau principal et réseau-hôtes pour les tiers et les appareils ménagers intelligents.
> Sauvegardez régulièrement vos données. Faites des sauvegardes une fois hors-ligne, par exemple sur un disque dur externe, et une fois en ligne, sur un cloud.

## Restez informé

Les cybercriminels sont créatifs et développent sans cesse de nouvelles stratégies et méthodes. Apprenez à connaître les derniers agissements des criminels sur Internet et les mesures à prendre:

Police cantonale bernoise
www.police.be.ch/cyber

Centre national pour la cybersécurite
www.ncsc.admin.ch

Cybercrimepolice,
www.cybercrimepolice.ch (en allemand)

iBarry – La plateforme pour la sécurité en ligne,
www.ibarry.ch

Card Security – Sécurité des cartes sur les boutiques en ligne, www.card-security.ch

Prévention suisse de la criminalité,
www.skppsc.ch

**Police cantonale bernoise**
Waisenhausplatz 32
3011 Berne

police.be.ch/cyber