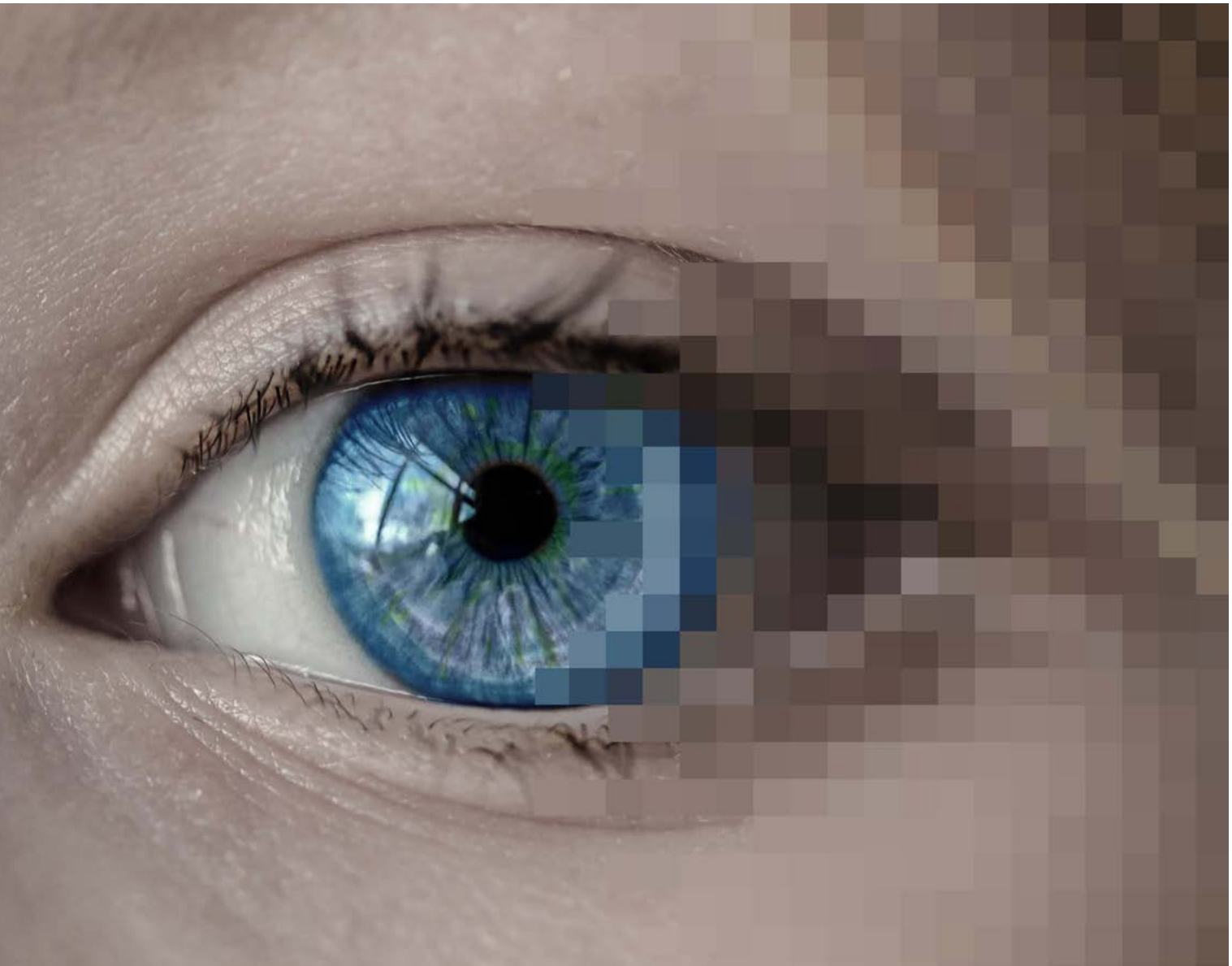
POLICE

Les quatre piliers de la cybersécurité
Informations pour les particuliers



Différentes mesures techniques doivent être prises et un bon comportement adopté pour se protéger de cyberattaques. Les quatre conseils fondamentaux de prévention suivants vous aideront à relever votre sécurité sur Internet et à maîtriser les attaques.

1 Restez informé

Informez-vous des agissements criminels sur Internet et des mesures de protection adéquates. Vous pouvez le faire sur les sites suivants:

> Police cantonale bernoise, www.police.be.ch/cyber
> Centre national pour la cybersécurité, www.ncsc.admin.ch
> Cybercrimepolice, www.cybercrimepolice.ch (en allemand)
> iBarry, www.ibarry.ch
> Prévention suisse de la criminalité (PSC), www.skppsc.ch/fr

2 Ne vous laissez pas duper

Protégez vos données d'accès
Ne divulguez jamais d'informations confidentielles et de données comme des mots de passe ou des informations sur votre carte de crédit par des canaux non personnels. C'est également valable pour les formulaires que vous avez ouverts en cliquant sur un lien dans un courriel, un SMS ou un média social. Les services sérieux ne vous solliciteront jamais par le biais d'un courrier électronique, d'un SMS ou par téléphone, pour vous demander des mots de passe ou des données sur votre carte de crédit.

Ne vous laissez pas mettre sous pression
Les criminels utilisent les émotions comme la peur, la curiosité ou la confiance pour par exemple vous soutirer des informations personnelles ou vous inciter à effectuer un virement. Dans bien des cas, l'escroc vous met sous pression. Ne répondez pas aux demandes d'argent ou de valeurs. En cas de doute, raccrochez le téléphone ou effacez les messages indésirables. Annoncez les prises de contact suspectes à la police.

Refusez l'accès
Les criminels peuvent se faire passer par exemple pour une collaboratrice ou un collaborateur d'une entreprise d'informatique, d'une banque ou de la police. Ne donnez jamais à personne l'accès ou l'accès à distance à votre compte e-banking, à des données confidentielles ou à votre ordinateur.

Faites preuve de méfiance
Soyez sceptique envers les offres de rendement lucratives, les chances de gains importants ou les bonnes affaires. Les promesses de gains importants et simples en un temps éclair ou les offres très bon marché sont typiquement «trop belles pour être vraies». La prudence est également de mise lorsqu'on vous parle du grand amour et que l'on vous demande ensuite une aide financière.

Modérez vos publications d'informations personnelles sur Internet (p. ex. les réseaux sociaux). Les criminels les collectent pour se préparer à vous attaquer.

3 Protégez vos systèmes et vos données

Utilisez des mots de passe sûrs
Un mot de passe devrait être composé d'au moins douze signes, dont des majuscules et minuscules, chiffres et caractères spéciaux. Dans l'idéal, il ne figure dans aucun dictionnaire, est généré au hasard et ne contient aucune information personnelle comme votre date de naissance. Une authentification à deux facteurs offre une protection supplémentaire. Important: créer un mot de passe pour chaque application. Un gestionnaire de mots de passe vous aidera à les gérer.

Veiller à garder un réseau protégé et des appareils actualisés
Beaucoup de nouveaux systèmes d'exploitation contiennent déjà un pare-feu intégré, un anti-virus et une fonction de mise à jour automatique. Activez les fonctions idoines pour chaque appareil de votre réseau.

Quelques fonctions de sécurité sont également déjà intégrées aux modems des fournisseurs d'accès Internet. Utilisez-les et informez-vous auprès de votre fournisseur en cas de doute.

La sécurité peut encore être relevée lorsque d'autres composants de sécurité sont installés entre le modem et le réseau domestique, comme un routeur muni d'un système de détection et de prévention d'intrusion (IDS et IPS) ou de filtrage du Web (filtrage DNS). Plusieurs routeurs peuvent d'ailleurs gérer différents segments du réseau, comme le réseau pour les hôtes et le privé. Vous permettez ainsi aux personnes qui vous rendent visite ou aussi aux appareils ménagers connectés d'accéder à Internet sans mettre votre réseau principal en danger. Utilisez ces paramètres.

Les systèmes de gestion intégrée des menaces «Unified Threat Management» offrent des solutions all-in-one. Ces solutions de sécurité complètes existent en matériel, logiciel ou sur le nuage (cloud).

Sécurisez vos données
Plusieurs systèmes d'exploitation intègrent déjà des solutions de sauvegarde. Ces solutions sont faciles à utiliser et sécurisent les données en permanence. Mais parce que les utilisatrices et les utilisateurs les laissent souvent connectées aux ordinateurs, cela les rend sensibles aux attaques cryptées. Archivez donc une copie séparée de votre sauvegarde (hors ligne) et une de plus sur le nuage (ailleurs qu'à la maison). Vérifiez régulièrement que vos données soient bien sauvegardées et qu'elles peuvent être restaurées.

4 Ce que vous pouvez faire en cas de sinistre

Premiers secours lors d'une cyberattaque
Débranchez immédiatement chaque système du réseau / d'Internet et n'oubliez pas de débrancher le WLAN. Appelez le numéro d'urgence 112 ou contactez un poste de police à proximité de chez vous (www.suisse-epolice.ch). Ne redémarrez pas le système avant que la police n'ait mis les traces en sûreté.

Chaque annonce compte
Annoncez à la police les cas relevant du droit pénal, comme le piratage, le vol ou le chantage, aussi vite que possible. En particulier lorsque vous avez subi un dommage.

Si aucun dommage n'a été subi, vous pouvez aussi annoncer le cas au Centre national pour la cybersécurité (www.ncsc.admin.ch).

Chaque dénonciation et chaque annonce peut fournir des indices décisifs sur son auteur.

Allez chercher de l'aide
Les conséquences d'un acte criminel peuvent représenter une charge financière et/ou psychique. N'hésitez pas à aller chercher de l'aide professionnelle pour digérer votre expérience. Un appel à une organisation d'entraide peut être un premier pas. Vous trouverez, par exemple, plusieurs services de conseil sur le site www.aide-aux-victimes.ch pour le canton de Berne.

Police cantonale bernoise
Waisenhausplatz 32
3011 Berne

police.be.ch