Linus Technologies
Sécurité numérique · Savoie

GUIDE PRATIQUE · GRATUIT

Les 10 réflexes qui protègent vos comptes

Dix mesures simples, applicables ce soir, sans rien acheter et sans connaissance technique. Elles ferment la plupart des portes par lesquelles les attaques passent réellement.

Pour les particuliers, les familles, les indépendants, les écoles, les mairies et les associations.

www.linustechnologies.fr

Les 10 réflexes

01 Un mot de passe unique par compte

Un seul site piraté suffit : le même couple adresse / mot de passe est ensuite essayé automatiquement partout ailleurs. Impossible à tenir de tête — c'est le rôle d'un gestionnaire de mots de passe. Vous n'en mémorisez plus qu'un seul.

02 La double authentification partout

Même volé, un mot de passe seul ne suffit plus. À activer d'abord sur votre messagerie : c'est elle qui commande la réinitialisation de tous vos autres comptes. Pensez à mettre les codes de secours à l'abri.

03 Une phrase plutôt qu'un mot

Quatre ou cinq mots sans lien entre eux résistent bien mieux qu'un mot court bardé de caractères spéciaux — et se retiennent sans effort.

04 Mettre à jour sans attendre

Téléphone, ordinateur, box, navigateur. Les failles corrigées sont rendues publiques : un appareil en retard de plusieurs mois est une porte dont la clé circule. Les mises à jour de sécurité se posent dans la semaine.

05 Ne jamais agir dans l'urgence

Un message ou un appel qui vous presse est un signal d'alerte, pas une raison de se dépêcher. On raccroche, et on rappelle le numéro officiel au dos de la carte bancaire ou sur le site que l'on connaît.

Les 10 réflexes (suite)

06 Vérifier l'adresse, pas le logo

Un logo se copie en trois secondes. Le nom de domaine, lui, ne ment pas : lisez-le en entier, caractère par caractère, avant de saisir quoi que ce soit.

07 Trois copies, deux supports, une ailleurs

Une copie sur l'appareil, une sur un disque externe débranché, une hors du domicile. Et un test de restauration une fois par an : une sauvegarde jamais restaurée n'est pas une sauvegarde.

08 Verrouiller et chiffrer

Code ou empreinte sur le téléphone, verrouillage automatique de l'écran, chiffrement du disque. Cela protège aussi en cas de simple perte, qui est le cas le plus fréquent.

09 Publier moins

Date de naissance, nom du chien, école des enfants, photo du billet d'avion : c'est le matériau des questions secrètes et des arnaques ciblées.

10 Savoir qui appeler

Avant l'incident, pas pendant. Une fiche avec les bons numéros près de l'ordinateur fait gagner des heures, et parfois beaucoup d'argent. Les numéros utiles sont en dernière page.

Si c'est déjà arrivé

1 Couper, sans tout casser

Déconnectez l'appareil d'Internet s'il est touché — mais ne le réinitialisez pas : vous effaceriez les traces utiles à la plainte.

2 Reprendre la messagerie en premier

C'est la clé de tous les autres comptes. Changez le mot de passe depuis un appareil sain, vérifiez les règles de transfert ajoutées à votre insu, déconnectez les sessions.

3 Prévenir la banque

Opposition et contestation écrite. En cas de paiement non autorisé, la réglementation européenne encadre le remboursement : il faut écrire, vite, et garder une trace.

4 Conserver les preuves

Captures d'écran, messages reçus, relevés, horaires. Tout ce qui est gardé sert au dépôt de plainte et aux démarches auprès des plateformes.

5 Signaler et se faire aider

Les dispositifs ci-dessous sont publics, gratuits et compétents.

Les numéros à garder sous la main

17Cyber	17cyber.gouv.fr Diagnostic en ligne et mise en relation avec un policier ou un gendarme.
Cybermalveillance	cybermalveillance.gouv.fr Assistance, fiches pratiques et annuaire de prestataires.
3018	Appel et application gratuits Cyberharcèlement des mineurs. Écoute, conseil, signalement accéléré.
Pharos	internet-signalement.gouv.fr Signaler un contenu ou un comportement illicite en ligne.
SignalConso	signal.conso.gouv.fr Site marchand douteux, arnaque commerciale, abonnement forcé.
CNIL	cnil.fr Vos droits sur vos données : accès, rectification, effacement.

Besoin d'un coup de main pour les mettre en place ?

Le bilan de sécurité consiste exactement à cela : passer ces dix points en revue avec vous, sur vos propres appareils. Premier échange gratuit.

07 66 22 81 99 · linustechnologies@outlook.com · www.linustechnologies.fr