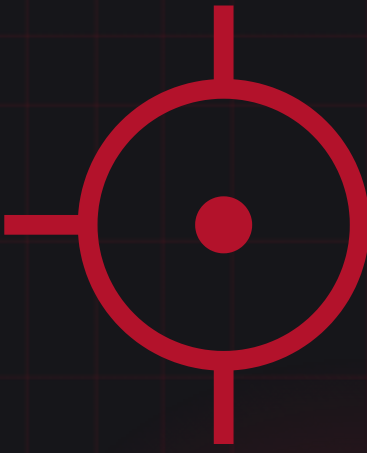
FORMATIONPREVENTION

GUIDE DES BONS RÉFLEXES

Prévenir les pièges du quotidien

12 thèmes, les gestes qui protègent votre entreprise. À garder à portée de main.



AVANT DE COMMENCER

Trois réflexes valables partout

1

Prenez une pause

L'urgence, la peur ou une récompense trop belle sont les leviers préférés des escrocs. Une demande pressante mérite justement qu'on ralentisse.

2

Vérifiez par un autre canal

Rappelez la personne ou l'entreprise au numéro que vous connaissez déjà, jamais à celui indiqué dans le message.

3

Signalez tout de suite

Au service informatique ou à votre responsable, même en cas de simple doute, et même si vous avez déjà cliqué.

Ce guide résume les 12 modules de Formation Prevention. Il ne remplace pas les modules : il vous les rappelle, thème par thème.

FORMATIONPREVENTION

THÈME 01 / 12

Phishing

> Un e-mail, un SMS ou un code QR piégé soigne tout ce que vous voyez : le nom de l'expéditeur, le logo, le ton. Ce qui le trahit est caché.

- **Regardez l'adresse réelle**

  Le nom affiché se choisit librement. Lisez l'adresse complète de l'expéditeur, et survolez un lien (appui long sur téléphone) pour voir où il mène vraiment.

- **Méfiez-vous de l'urgence**

  Colis retenu, compte bloqué, facture impayée : un délai très court est un signal d'alerte, pas une raison d'agir vite.

- **Tapez l'adresse vous-même**

  Pour vous connecter à votre banque ou à un service, saisissez l'adresse que vous connaissez au lieu de suivre le lien reçu.

- **Codes QR**

  Ne scannez pas un code QR collé sur un parcmètre ou reçu par courrier sans vérifier l'adresse qu'il ouvre.

À RETENIR

Message suspect : ne cliquez pas, ne répondez pas, ne le transférez pas à un collègue. Signalez-le au service informatique ou à reports@antiphishing.ch.

THÈME 02 / 12

Usurpation d'identité

> Un faux directeur, fournisseur ou fiduciaire demande un virement urgent et confidentiel, ou un changement de coordonnées bancaires.

- **Rappelez au numéro connu**
  Contactez la personne par un numéro que vous aviez déjà, jamais celui donné dans le message ou l'appel.
- **Respectez la procédure**
  Un paiement inhabituel passe par le double contrôle prévu, même si le « directeur » exige le secret.
- **Changement d'IBAN**
  Toute demande de modification des coordonnées bancaires d'un fournisseur se vérifie par téléphone avant d'être enregistrée.
- **Lisez le domaine**
  Une seule lettre de différence dans l'adresse de l'expéditeur suffit à l'escroc.

À RETENIR

Urgence, secret et paiement réunis : arrêtez-vous et vérifiez. Personne ne vous reprochera d'avoir vérifié.

THÈME 03 / 12

Mots de passe

> Un mot de passe court ou réutilisé tombe vite, et ouvre alors tous les comptes qui l'utilisent.

- **La longueur d'abord**
  12 caractères au minimum, 16 ou plus de préférence. Une phrase facile à retenir vaut mieux qu'un mot compliqué.
- **Un mot de passe par compte**
  Si un site se fait voler ses données, vos autres comptes restent protégés.
- **Un gestionnaire de mots de passe**
  Il crée et retient pour vous des mots de passe solides : celui fourni par votre entreprise, ou par exemple Bitwarden ou Proton Pass.
- **Rien de personnel**
  Ni prénom, ni date de naissance, ni nom de l'entreprise, ni année : ce sont les premiers essais d'un pirate.

À RETENIR

Un seul mot de passe à vraiment retenir : celui du gestionnaire. Rendez-le long et unique.

THÈME 04 / 12

Double authentification

> Avec un second facteur, un mot de passe volé ne suffit plus pour entrer dans votre compte.

- **Activez-la partout**
  Messagerie, gestionnaire de mots de passe, comptes professionnels : partout où c'est proposé.
- **Préférez une application**
  Une application d'authentification ou une clé de sécurité protège mieux qu'un code reçu par SMS.
- **Ne donnez jamais un code**
  Ni le service informatique ni une banque ne vous le demandera, par téléphone ou par message.
- **Refusez ce que vous n'avez pas demandé**
  Des demandes de connexion à répétition signifient que quelqu'un a votre mot de passe : refusez, changez-le et prévenez le service informatique.

À RETENIR

Rangez vos codes de récupération dans votre gestionnaire de mots de passe, pas dans un e-mail.

THÈME 05 / 12

Navigation web

> Un faux site peut être identique au vrai, cadenas compris.

- **Le cadenas ne suffit pas**
  Il chiffre la connexion, il ne dit rien de l'honnêteté du site. Lisez l'adresse complète.
- **Attention aux annonces**
  Dans les résultats de recherche, les liens sponsorisés peuvent être payés par des escrocs : tapez plutôt l'adresse officielle.
- **Téléchargements officiels**
  Installez un programme uniquement depuis le site de son éditeur, ou demandez au service informatique.
- **Fausses alertes**
  Une alerte virus avec compte à rebours ou numéro à appeler est un piège : fermez l'onglet. Un avertissement de certificat ne s'ignore pas.

À RETENIR

En cas de doute sur une page, fermez-la et passez par l'adresse que vous connaissez.

THÈME 06 / 12

Wi-Fi public

> Au café, à la gare ou à l'hôtel, quelqu'un peut se faire passer pour le réseau officiel et voir passer ce que vous envoyez.

- **Votre téléphone d'abord**
  Le partage de connexion de votre téléphone est plus sûr qu'un réseau ouvert.
- **Le VPN de l'entreprise**
  Activez-le avant de travailler sur un réseau que vous ne maîtrisez pas.
- **Pas d'opérations sensibles**
  Évitez l'e-banking et les données confidentielles sur un réseau public.
- **Pages de connexion piégées**
  Une page qui réclame une carte bancaire ou l'installation d'un programme pour accéder au Wi-Fi : refusez. Oubliez le réseau après usage.

À RETENIR

Un mot de passe affiché au comptoir ne fait pas d'un réseau partagé un réseau privé.

THÈME 07 / 12

Ransomware

> Un rançongiciel chiffre les fichiers de l'entreprise et exige une rançon. Il entre souvent par une pièce jointe piégée.

- **N'activez pas le contenu**

  Un document reçu par e-mail qui demande d'« activer le contenu » pour s'afficher est un signal d'alerte.

- **Écran bloqué ou fichiers renommés**

  Coupez tout de suite la connexion réseau (câble et Wi-Fi), puis prévenez le service informatique et votre responsable.

- **Ne payez pas**

  Et ne contactez pas les pirates : payer ne garantit ni la récupération des fichiers, ni que les données ne seront pas publiées.

- **Ne branchez pas la sauvegarde**

  Le disque de sauvegarde serait chiffré à son tour. Laissez le service informatique décider de la suite.

À RETENIR

Couper le réseau, puis prévenir : deux gestes, dans cet ordre.

THÈME 08 / 12

Clés USB et supports

> Une clé trouvée ou offerte peut contenir un programme malveillant, ou même se faire passer pour un clavier qui tape des commandes.

- **Jamais de clé inconnue**

  Une clé trouvée, reçue par la poste ou offerte sur un salon ne se branche pas : remettez-la au service informatique.

- **Des clés chiffrées**

  Pour les données professionnelles, utilisez les supports chiffrés fournis par l'entreprise, pas une clé personnelle.

- **Supprimer n'efface pas**

  Supprimer des fichiers ou formater rapidement ne les efface pas vraiment : confiez les supports usagés au service informatique.

- **Support perdu**

  Une clé ou un disque perdu avec des données de l'entreprise se signale aussitôt.

À RETENIR

Vous avez branché un support douteux : débranchez-le, coupez le réseau et prévenez.

THÈME 09 / 12

Télétravail

> À la maison, la box Internet et l'ordinateur de travail sont votre première protection.

- **Réglez votre box**
  Changez le mot de passe d'administration d'origine, choisissez WPA3 (au minimum WPA2) et un mot de passe Wi-Fi d'au moins 16 caractères, idéalement 20.
- **Un réseau invités**
  Pour les visiteurs et les objets connectés, séparés de votre ordinateur de travail.
- **Un ordinateur pour le travail**
  Réservé au travail, mis à jour, et verrouillé dès que vous vous levez. Accès aux données par le VPN de l'entreprise.
- **Discrétion**
  Appels confidentiels et écran à l'abri des regards, documents rangés.

À RETENIR

Ordinateur perdu ou volé : prévenez immédiatement le service informatique.

THÈME 10 / 12

Deepfake et vishing

> Une voix peut être imitée à partir de quelques secondes d'enregistrement, un visage en visioconférence aussi, et le numéro affiché peut être falsifié.

- **Raccrochez et rappelez**

  Au numéro que vous connaissez, même si la voix est celle de votre directeur.

- **Jamais de code par téléphone**

  Ni mot de passe, ni code reçu par SMS, ni PIN, quel que soit l'interlocuteur.

- **Pas de prise de contrôle**

  Refusez d'installer un programme ou de laisser un inconnu (faux support, fausse police) contrôler votre ordinateur.

- **Le comportement compte plus que l'apparence**

  Demande inhabituelle, pression, secret : ce sont ces signes qu'il faut écouter.

À RETENIR

Un doute pendant un appel : mettez fin à la conversation. Le vrai interlocuteur comprendra.

THÈME 11 / 12

Sauvegardes et fichiers sensibles

> Panne, incendie, rançongiciel : sans sauvegarde à jour et à l'abri, le travail est perdu.

- **La règle 3-2-1**

  Trois copies des données, sur deux supports différents, dont une dans un autre lieu (recommandation de l'OFCS).

- **Une copie hors ligne**

  Débranchez le disque après chaque sauvegarde, et testez régulièrement la restauration.

- **Partager avec mesure**

  Un fichier sensible se partage avec les seules personnes concernées, jamais par un lien ouvert à tous.

- **Mauvais destinataire**

  Un document envoyé à la mauvaise personne se signale tout de suite : l'entreprise peut avoir des obligations légales.

À RETENIR

Une sauvegarde qu'on n'a jamais restaurée n'est qu'un espoir.

THÈME 12 / 12

Signalement d'incident

> Chaque minute compte : plus l'entreprise est prévenue tôt, plus l'attaque est arrêtée tôt.

- **Tout de suite**
  Signalez dès que vous avez un doute, même pour un incident évité de justesse.
- **Par téléphone de préférence**
  Votre messagerie est peut-être déjà entre de mauvaises mains.
- **Dites l'essentiel**
  L'heure, ce qui s'est passé, le compte ou le message concerné, et ce que vous avez déjà fait.
- **Ne supprimez rien**
  Et ne minimisez pas : ce sont des indices précieux pour le service informatique.

À RETENIR

Signaler vite n'est jamais une erreur.

EN CAS D'INCIDENT

Les quatre gestes

1. **Arrêtez**
   Ne cliquez plus, ne répondez plus, ne saisissez plus rien.
2. **Isolez**
   Si l'ordinateur semble infecté, coupez la connexion réseau (câble et Wi-Fi).
3. **Prévenez**
   Le service informatique et votre responsable, par téléphone de préférence.
4. **Racontez**
   L'heure, ce qui s'est passé, ce que vous avez fait. Ne supprimez rien.

VOS CONTACTS

Service informatique _____

Responsable _____

Téléphone d'urgence _____

EN SUISSE

Signaler un phishing
reports@antiphishing.ch

Office fédéral de la cybersécurité (OFCS)
www.bacs.admin.ch

Préjudice financier
Votre police cantonale

FORMATIONPREVENTION

FORMATION PREVENTION

Se former en le vivant

Des modules d'environ 10 minutes, des mises en situation réalistes et des exemples suisses, pour que les bons réflexes deviennent des habitudes.

formation-prevention.ch

IMPRESSUM

Datalys
Grand Rue 8
1196 Gland
Suisse

© 2026 Datalys