Les collaboratrices et collaborateurs au cœur de la sécurité

Guide pratique de cybersécurité pour les PME

Auteur : Maillard Marcel - Consultant stratégique
Mandants : Juranet.ch, jsih.ch, batico.ch

www.juranet.ch
LE PORTAIL JURASSIEN

JURA INDUSTRIEL HORLOGER
www.jsih.ch

BATICO
ARTISANAT • BÂTIMENT • CONSTRUCTION

Sommaire

1. Introduction – Les PME, cibles privilégiées des cybercriminels
2. Dix réflexes essentiels pour se protéger au quotidien
3. Pourquoi sensibiliser son personnel ?
4. Former, informer, simuler : la triple approche efficace
5. Instaurer une culture de la sécurité
6. Huit règles d'or du comportement numérique
7. Check-list
8. Conclusion – De la vigilance individuelle à la sécurité collective

1. Introduction
Les PME, cibles privilégiées des cybercriminels

Les petites et moyennes entreprises (PME) sont des cibles de choix pour les cybercriminels : chaînes d'approvisionnement, sous-traitance, manque de ressources dédiées…

Les attaques visent avant tout les comportements à risque.

Renforcer la sécurité technique est nécessaire, mais la résilience d'une PME repose d'abord sur les réflexes des collaboratrices et collaborateurs.

Ce livre blanc propose une démarche pragmatique, visuelle et actionnable pour instaurer des habitudes simples et efficaces.

OBJECTIF DU GUIDE

Aider les PME à structurer un programme de sensibilisation continue, avec des messages clairs, des formations régulières, des simulations maîtrisées et une culture de sécurité partagée par toutes et tous.

2. Dix réflexes essentiels pour se protéger au quotidien

- Vérifier les liens dans les e-mails envoyés par des inconnus.
- Ne pas partager d'informations personnelles/sensibles avec des inconnus (y compris sur les réseaux sociaux).
- Effectuer des achats uniquement sur des sites commerciaux connus.
- Effectuer des sauvegardes régulières des données.
- Réaliser des mises à jour logicielles régulières sur les appareils (y compris mobiles).
- Utiliser des mots de passe forts et un gestionnaire de mots de passe.
- Activer l'authentification à deux ou plusieurs facteurs.

- N’utiliser le Wi-Fi public qu’en cas de nécessité et avec un VPN.
- S’informer auprès de sources fiables uniquement.
- Signaler les cas de fraude à la police et aux référents internes.

Pourquoi ces réflexes comptent ?

Ces bonnes pratiques visent à réduire la surface d’attaque humaine : elles permettent de repérer les tentatives de phishing, de limiter l’impact d’un incident par la sauvegarde et de renforcer l’authentification des comptes critiques.

3. Pourquoi sensibiliser son personnel ?

Former régulièrement le personnel consiste à attirer l’attention sur les risques liés aux cyberattaques et à développer la capacité à détecter les fraudes (hameçonnage, rançongiciels, ingénierie sociale). Des collaboratrices et collaborateurs informés réagissent correctement, ce qui réduit les risques et évite les situations mettant en péril la sécurité des données et l’intégrité des processus métier.

L’ESSENTIEL EN BREF

- Organiser régulièrement des formations.
- Informer fréquemment le personnel des menaces et tendances du moment.
- Organiser des simulations d’attaques par hameçonnage.
- Instaurer une culture de la sécurité.

4. Former, informer, simuler : la triple approche efficace

Proposer des formations

Proposez des formations régulières couvrant les principales menaces (phishing, rançongiciels, ingénierie sociale), les indices d’e-mails/pièces jointes/liens suspects et les bonnes pratiques (mots de passe robustes, mises à jour, pare-feu et antivirus).

Simulation d'attaques par hameçonnage

Les campagnes de phishing simulé, menées à intervalles irréguliers, permettent d'entraîner les réflexes en situation. Les personnes qui cliquent sur des liens ou divulguent des informations sensibles reçoivent un feedback immédiat et des conseils ciblés.

5. Instaurer une culture de la sécurité

Promouvez une culture où la sécurité de l'information est une responsabilité collective. Ouvrez des canaux de signalement, valorisez les bons comportements, intégrez les directives de sécurité dans les processus et faites des cadres des modèles de comportement.

BON À SAVOIR

Adoptez des messages courts et réguliers (affiches, messages internes, micro-learning) plutôt que de longues campagnes annuelles : l'apprentissage en continu renforce la vigilance.

6. Huit règles d'or de la sécurité de l'information

Une petite erreur peut avoir de lourdes conséquences (système infecté, vol de données, pertes financières). Ces huit règles soutiennent un usage adéquat des données et de l'infrastructure informatique :

1

Mots de passe forts

- Utiliser des mots de passe robustes (majuscules, minuscules, chiffre, caractère spécial).
- Ne jamais partager ses mots de passe.
- Changer le mot de passe s'il est compromis.
- Ne pas noter ses mots de passe sur des supports non protégés.
- Conserver les accès en lieu sûr (gestionnaire de mots de passe).
- Un mot de passe différent pour chaque compte (pro/perso).

2 Place de travail

- Ne laisser aucun document sensible sans surveillance.
- En cas d'absence, entreposer les documents dans un espace sécurisé.
- Verrouiller sa session dès qu'on s'éloigne.
- Éteindre l'ordinateur en fin de journée.
- Utiliser l'impression sécurisée (PIN/badge) et récupérer immédiatement.

Protection de l'information 3

- Séparer données privées et données professionnelles.
- Ne pas stocker de documents de l'entreprise sur des appareils privés.
- Enregistrer les documents sur les serveurs de l'entreprise.
- Appliquer les directives de classification des données.
- Séparer les stockages (cloud/SSD) et éviter les clés USB non contrôlées, les clés USB doivent être testées avant usage sur un poste d'entreprise.
- Ne laisser aucun équipement non protégé sans surveillance.
- Attention aux outils IA, traducteurs et réseaux sociaux.
- Eviter tout partage d'information non publique ou sensible sur Internet et réseaux sociaux.

4 Pratiques sociales

- Vérifier l'identité de toute personne demandant des informations.
- Rester vigilant lors des échanges téléphoniques, e-mails, réunions avec des tiers.
- En cas de doute, rappeler directement l'entreprise par des coordonnées vérifiées.
- Signaler immédiatement toute tentative de pression inhabituelle.

Internet 5

- Vérifier la destination d'un lien avant de cliquer.
- Ne pas exécuter/ouvrir de fichiers téléchargés d'origine douteuse.
- Toute donnée publiée en ligne peut rester accessible indéfiniment.
- Ne jamais partager de fichiers contenant des informations sensibles via des sites non approuvés.

6 Messagerie et emails : la prudence est de mise

- Communiquer son adresse e-mail pro uniquement à des tiers/sites liés au travail.
- Usage privé de la messagerie : modération.
- Ne pas transférer d'e-mails/document pro vers l'adresse personnelle.
- Ne pas ouvrir de pièce jointe/cliquer sur un lien en cas de provenance suspecte.
- Activer le chiffrement pour les messages confidentiels.
- Vérifier l'expéditeur et le ton du message.
- Ne jamais céder à la pression d'un inconnu ou communiquer des identifiants.
- Ne pas ouvrir de pièces jointes ni cliquer de liens en cas de doute.
- Aucune banque/assureur ne demande des données sensibles par e-mail ou SMS.
- Se méfier des messages imitant des marques connues.

Mobilité 7

- Installer un filtre de confidentialité sur l'ordinateur portable utilisé en public.
- Activer le verrouillage d'écran (PIN/mot de passe) sur le téléphone.
- Éviter la veille pendant le transport ; préférer l'extinction ou l'hibernation.
- Éviter les Wi-Fi publics ou utiliser un VPN.

8 Agir en cas de doute

- Signaler tout e-mail, doute, erreur commise au référent sécurité dans les plus brefs délais.
- Déclarer immédiatement tout vol/perte d'équipement.
- Signaler tout comportement suspect à un responsable.
- En cas de cyberharcèlement : collecter des preuves, bloquer l'auteur et alerter.

7. Check-list personnel - À vérifier chaque mois

- Mises à jour effectuées (PC, mobile, logiciels).
- Sauvegardes vérifiées et restaurations testées.
- Mots de passe revus périodiquement.
- Aucun document sensible hors des espaces approuvés.
- Signalement de tout e-mail ou comportement suspect.

CONCLUSION

De la vigilance individuelle à la sécurité collective

La sécurité ne se décrète pas, elle se pratique.

En ancrant les bons réflexes, en formant régulièrement les équipes et en valorisant la vigilance, les PME se dotent d'une véritable armure collective.

Chaque geste compte.

Ce guide vous est offert par

www.juranet.ch
LE PORTAIL JURASSIEN

JURA INDUSTRIEL HORLOGER
www.jsih.ch

BATICO
ARTISANAT • BÂTIMENT • CONSTRUCTION