Help Protect Your POS Payment Terminal from Fraud

Help Protect Your POS Payment Terminal from Fraud

Point-of-Sale (POS) fraud occurs during in-person transactions in your shop or store. It involves a fraudster interacting with you or your employees in your workplace instead of online or on the phone. The good news is that there are steps you can take to help prevent in-store scams

Check for Approved Transactions

Ensure every transaction shows as successfully completed on your POS payment terminal and merchant receipt.

Safeguard Your POS Payment Terminal and Use Strong Passwords

- Safeguard your password when entering it into your POS payment terminal in the presence of a customer.
- Use complex passwords to sign into your POS payment terminal and change them regularly, including when an employee leaves your company.
- It is strongly recommended that certain functions, such as refunds, be protected with a password.
- Only authorize a limited number of employees to access your POS payment terminal.

Safeguard the Location of Your POS Payment Terminal

- Watch for people hovering around your POS payment terminal without making a purchase.
- If possible, secure your POS payment terminal to your counter or service desk with security cables to reduce the chance that someone could swap your equipment with another payment terminal.
- Install surveillance cameras around the area where customers make payments.
- Lock your POS payment terminal away securely at night.

Train Your Employees on POS Payment Terminal Tampering

Help your frontline employees protect your business by training them to recognize signs of POS payment terminal tampering (please refer to your POS payment terminal manual for details) and ensure they verify POS payment terminal service and repair technicians who visit your store. Personally inspect your POS payment terminal for tampering periodically.

Keep Your Business Bank Account Profile Up to Date

Review your business bank account profile to ensure, for example, that your authorized employee list is up to date. Immediately remove access for those employees who no longer work for you.

Secure Your Store's Wi-Fi

- Never use public or unsecured Wi-Fi networks with a POS payment system.
- Change the manufacturer's default password for your store's Wi-Fi network.
- Ensure your store's Wi-Fi is password protected with a strong, complex password that is not shared with customers or employees.
- Frequently change the password.
- Install a firewall on Wi-Fi networks for additional security and scan periodically for unauthorized Wi-Fi networks that may have been set up without your knowledge.

Want More Ways to Help Protect Yourself from Fraud?

Scan the QR code or visit
tdmerchantsolutions.com/fraud
for best practices and a little peace of mind.

599679 (0924)

Aidez à protéger votre terminal PDV contre la fraude

Aidez à protéger votre terminal PDV contre la fraude

La fraude au terminal point de vente (PDV) se produit lors d'opérations en personne dans votre commerce : un fraudeur interagit avec vous ou vos employés sur votre lieu de travail plutôt qu'en ligne ou au téléphone. La bonne nouvelle, c'est que vous pouvez prendre des mesures pour prévenir les arnaques en magasin.

Vérifier que l'opération a été approuvée

Assurez-vous que votre terminal PDV et le reçu du commerçant indiquent que l'opération a bien été traitée.

Protéger votre terminal PDV et utiliser des mots de passe solides

- Protégez votre mot de passe lorsque vous l'entrez dans votre terminal PDV en présence d'un client.
- Utilisez des mots de passe complexes pour ouvrir une session dans votre terminal PDV et modifiez-les régulièrement, y compris lorsqu'un employé quitte votre entreprise.
- Il est fortement recommandé que certaines fonctions, telles que les remboursements, soient protégées par un mot de passe.
- N'autorisez l'accès à votre terminal PDV qu'à un nombre limité d'employés.

Protéger l'emplacement de votre terminal PDV

- Gardez un œil sur les personnes qui tournent autour de votre terminal PDV sans faire d'achat.
- Dans la mesure du possible, fixez votre terminal PDV à votre comptoir ou bureau de service au moyen de câbles de sécurité pour réduire le risque que quelqu'un remplace votre équipement par un autre terminal de paiement.
- Installez des caméras de surveillance autour de la zone où les clients effectuent leurs paiements.
- Rangez votre terminal PDV de façon sécuritaire la nuit.

Former vos employés sur l'altération des terminaux PDV

Aidez vos employés de première ligne à protéger votre entreprise en les formant afin de reconnaître les signes d'altération des terminaux PDV (consultez le manuel de votre terminal PDV pour en savoir plus) et assurez-vous qu'ils vérifient l'identité des techniciens de maintenance et de réparation de terminal PDV qui se présentent dans votre commerce. Inspectez personnellement votre terminal PDV de temps à autre pour vous assurer qu'il n'a subi aucune altération.

Tenir à jour le profil de votre compte des Services bancaires aux entreprises

Passez en revue le profil de votre compte des Services bancaires aux entreprises pour vous assurer, par exemple, que votre liste d'employés autorisés est à jour. Supprimez immédiatement l'accès des employés qui ne travaillent plus pour vous.

Sécuriser le réseau Wi-Fi de votre magasin

- N'utilisez jamais de réseaux Wi-Fi publics ou non sécurisés avec un système de paiement PDV.
- Changez le mot de passe par défaut du fabricant du réseau Wi-Fi de votre magasin.
- Assurez-vous que le réseau Wi-Fi de votre magasin est protégé par un mot de passe solide et complexe qui n'est pas connu de vos clients ou de vos employés.
- Changez fréquemment votre mot de passe.
- Installez un pare-feu sur les réseaux Wi-Fi afin de bénéficier d'une sécurité accrue et vérifiez périodiquement si des réseaux Wi-Fi non autorisés ont été configurés à votre insu.

Vous voulez connaître plus de façons de vous protéger contre la fraude?

Numérisez le code QR ou visitez solutionsauxcommercantstd.com/fraude pour découvrir des pratiques gagnantes et avoir l'esprit tranquille.

599679 (0924)