Contrôles recommandés pour les terminaux autonomes de point de vente

Gérant _____ Date _____

Vérifiez le terminal de point de vente

- ❑ Y a-t-il plus qu'une tête de lecture dans le lecteur de carte?
- ❑ La surface autour du lecteur de carte a-t-elle l'air d'avoir été essuyée?
- ❑ Le terminal a-t-il été trafiqué ou ouvert?
- ❑ Un port semble-t-il brisé (voir Figure 5A)?
- ❑ Si vos terminaux ont des scellés de sécurité, ceux-ci ont-ils été perforés ou semblent-ils plissés/pliés ou coupés?
- ❑ Votre terminal est-il au même endroit que la veille?

Vérifiez les alentours pour voir s'il n'y aurait pas de caméras miniatures dissimulées

- ❑ Y a-t-il des caméras pouvant servir à capter les NIP dans les endroits suivants?

- Dans le plafond (voir Figure 3A)
- Dans des murs, des plaques ou de l'affichage adjacents
- Dans des présentoirs à brochures ou des objets personnels
- Dans les présentoirs derrière la caisse
- Dans un paquet de cigarettes ou autre produit en vente à la caisse
- Au moins une fois la semaine, regardez derrière les panneaux du plafond, au-dessus du clavier-NIP, où une caméra pourrait être installée. Y-a-t-il des fils supplémentaires? Vérifiez les lieux d'entreposage, salles de toilettes et autres endroits peu fréquentés derrière l'aire de vente. Y a-t-il des fils supplémentaires? Y a-t-il des appareils d'enregistrement (DVD, joueur MP3, lecture USB, ou magnétoscopes)?

Suggestions pour accroître la sécurité

- Si possible, verrouillez le terminal de PDV à la fin de la journée
- Protégez le terminal à l'aide d'un mot de passe et fermez-le chaque jour
- Notez le numéro de série du clavier-NIP et du terminal pour vous assurer que c'est le même que sur les appareils

Éduquez votre personnel

- ❑ Y a-t-il eu des distractions inhabituelles ? Avez-vous remarqué quoi que ce soit d'anormal ?
- ❑ Ne remettez le clavier-NIP à un client que pour que la personne effectue l'entrée de son NIP.
- ❑ Test du signe distinctif – certains commerçants marquent leurs claviers-NIP d'un signe distinctif pour les reconnaître facilement.

Vérifiez les caméras de surveillance

- ❑ Remarquez-vous quoi que ce soit de différent par rapport à l'enregistrement vidéo précédent?

Identification du personnel d'entretien

- ❑ Le personnel d'entretien a-t-il montré des pièces d'identité avant de manipuler l'appareil? Est-il arrivé à l'heure convenue? S'est-il présenté? La visite avait-elle quoi que ce soit d'inhabituel?
- ❑ Créez et maintenez des registres pour tous les appels et toutes les visites d'entretien.

Voyez au verso les indices visuels à rechercher...

POUR EN SAVOIR DAVANTAGE, COMMUNIQUEZ AVEC VOTRE ACQUÉREUR OU VOTRE FOURNISSEUR DE SERVICE

Indices visuels à rechercher...

PROTÉGEZ VOS CLAVIERS NIP

Soyez attentifs!

- Deux personnes ou plus magasinant ensemble
- Achat d'objets encombrants
- Remplacement du clavier-NIP par un faux clavier
- Sachez toujours où se trouve le clavier-NIP
- Voyez à sécuriser clavier-NIP quand il ne sert pas

Figure 1 : Vidéo montrant des fraudeurs en train de remplacer le clavier-NIP dans un commerce

Figure 2 : Les appareils de clonage de cartes peuvent être très petits. Cherchez sous les comptoirs et derrière les caisses. Ils peuvent même être portés par des employés.

Figure 3A : Caméras miniatures dissimulées dans le plafond.

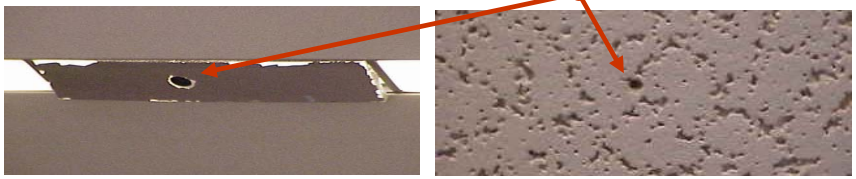

Figure 3B : Fils dans le plafond.

Figure 4 : Enregistreur de frappes. Cet appareil peut être branché à un clavier pour enregistrer toutes les frappes.

Figure 5A : Câble externe non autorisé/port brisé.

Figure 5B : Scellé de sécurité trafiqué.

Figure 5C : Après enlèvement des scellés de sécurité.

Que faire si vous découvrez quelque chose de suspect sur l'appareil ou à l'intérieur?

- Ne dérangez rien à la scène du crime possible.
- Transportez délicatement les claviers-NIP jusqu'à un endroit sûr.
- Communiquez immédiatement avec la police et votre acquéreur (Processus à déterminer par chaque commerçant: ça pourrait être la sécurité de votre employeur, la police locale et votre acquéreur).