

Putting the Spotlight on Secure Payments

Keeping up with the very latest security developments can seem a complex and daunting task. However, industry bodies like APACS, along with leading payment vendors like VeriFone, are playing a key role in helping casino and gaming business owners understand how best to ensure payment device security.

The casino and gaming market has traditionally been an industry based around cash. Now, the gambling industry is increasingly recognising the benefits of card and electronic payments as a platform for gaining greater efficiencies and enabling better customer analysis in order to increase competitiveness. However, along with that goes the need to ensure all electronic payment transactions taking place are secure.

In the UK, the introduction of chip and PIN has made it more difficult for fraudsters to commit fraud. However, to protect cardholder data from compromise, this year the Payment Card Industry (PCI) adopted new PED security requirements (PCI PED) designed to prevent and detect tampering incidents.

The new security requirements cover a variety of areas including tamper protection, PIN monitoring prevention, authentication of software applications, smart card reader security, as well as encryption.

Reducing the risk

Despite the arrival of the new PCI PED-approved systems, criminals continue to target less secure pre-PED devices, employing a variety of methods to physically compromise devices. These can include tampering with an in-store device, or obtaining the same device a business owner uses and installing a speciality software programme to capture debit or credit card details, before substituting the tampered device for the retailer's device.

Industry bodies such as APACS have created guidance on the strategies card-accepting businesses can employ to keep chip and PIN equipment safe and protected. These include ensuring the physical location of chip and PIN terminals is secure, to implementing good management routines for chip and PIN equipment, and putting in place standardised staff security processes.

APACS recommendations

In its guidelines APACS (www.apacs.org.uk) recommends the use of secure cradles to reduce the risk of terminal theft, along with the use of CCTV to cover the till area. To further protect the integrity of chip and PIN devices, APACS advises undertaking regular checks to ensure that both equipment and device cabling has not been tampered with.

Alongside creating an inventory management system to document serial numbers and locations (including replacements and spares), APACS advocates the regular review of inventories and asset management records.

Staff security is a further key area, and APACS recommends adopting a standardised recruitment and vetting procedure for all employees. When an employee leaves, their security related entitlements should be revoked.

Working together to protect cardholder information

To ensure business owners have a secure payment solution in place, VeriFone has developed a series of best practices. These recommendations include undertaking weekly visual inspections on devices and checking the electronic serial number matches that on the base of the device. If the payment device supports electronic serial numbers, this should be validated every time the POS starts up. In addition, device passwords should be changed immediately, as the factory set passwords can become widely known. Devices that consistently don't work properly (for example, high mag-strip read failures, or debit card declines) should be closely monitored.

Every instance in which a device is replaced should be tracked and any spares should be stored under lock and key to prevent unauthorised removal. The identity of every repair technician visiting the store should be verified and technicians should be accompanied by a store employee at all times.

To help fully understand what is required to protect cardholder data from compromise, VeriFone provides payment security information at www.verifone.com/security.

While chip and PIN device security standards become ever more rigorous, to prevent the risk of compromise, business owners need to implement comprehensive security best practices at the point of sale. As a champion of cardholder data security, VeriFone is committed to promoting security measures that can help all card-accepting businesses better protect themselves and their customers.

