Script - PCI Security Awareness Video

| **Graphic** | **English Text** | **Translation** |
| --- | --- | --- |
|  | This is a LUCY video covering the payment card industry (PCI) data security standards. |  |
|  | You will learn about the dangers od exchanging credit card details over the phone, internet or other mediums, and how to protect yourself and your company from fraud, identity theft and sata leaks. |  |
|  |  |  |
|  |  |  |
|  | There is good reason to be cautious where the PCI is concerned, as each year millions of payment card |  |
|  | Accounts are compromised through various security and data breaches worldwide. |  |
|  | If you happen to handle sensitive payment card information as part of your job, then you should be aware of the appropriate security measures you need to take to protect and secure cardholder data. |  |
|  |  |  |
|  |  |  |
|  | What are these data security standard (DSS) and why are they important? |  |
|  | The DSS is composed of 12 requirements that all merchants and payment processors must adhere to in order to protect customer data. |  |
|  |  |  |
|  | Non-compliance comes with penalties like fees, increased processing times and damage of trust between customer and company. |  |
|  |  |  |
|  | There are several most common practices that data thieves employ when attempting to steal payment card information. |  |
|  |  |  |
|  | These are:  Shoulder surfing is looking over someone’s shoulder to obtain their personal information. |  |
|  |  |  |
|  | Unauthorized physical access happens when a person enters a secure area without prior permission. |  |
|  | Eavesdropping occurs when a third party inadvertently listens in on a private conversation. |  |
|  | Phishing is the attempt to acquire payment card information illegally via fraudulent e-mail and social media messages. |  |
|  |  |  |
|  | Social engineering refers to a myriad of manipulative techniques used to make you reveal sensitive and personal information about yourself or others. |  |
|  |  |  |
|  | Always be careful when handling customer data as you never know who may be watching, listening or trying to manipulate you. |  |
|  |  |  |
|  | An important part of protecting carholder data is understanding the security features that are built into every payment card. |  |
|  |  |  |
|  | These include: Logos nad holograms |  |
|  | Embosed payment card numbers |  |
|  | Expiration dates |  |
|  | Signature panels |  |
|  | Card security codes |  |
|  | So what are those 12 DSS requirements? |  |
|  | 1. Install and maintain a firewall configuration to protect cardholder data. |  |
|  | 1. Do not use vendor-supplied defaults for system passwords and other security parameters. |  |
|  | 1. Protect stored cardholder data, such as authentication data and primary account numbers. |  |
|  | 1. Encrypt transmission of cardholder data across open, public networks. |  |
|  | 1. Use and regularly update antivirus software. |  |
|  | 1. Develop and maintain secure systems and applications. |  |
|  | 1. Restrict access to cardholder data by business nees-to-know. |  |
|  | 1. Assign a unique ID to each person with computer access. |  |
|  | 1. Restrict physical access to cardholder data. |  |
|  | 1. Track and monitor all access to network resources and cardholder data. |  |
|  | 1. Regularly test security systems and processes. |  |
|  | 1. Maintain a policy that addresses information security |  |
|  | and maintain a formal security awareness program. |  |
|  | The PCI DSS requirements emphasize the protection of cardholder’s data at its three most vulnerable points: |  |
|  | Retention |  |
|  | Access |  |
|  | Distribution |  |
|  | Retention. You may retain only cardholder data needed for business, legal, or regulatory purposes. |  |
|  | Do not retain the card’s security code, the cardholder’s PIN or the card’s full magnetic strip data. |  |
|  | Access. Protect cardholder data by allowing access only to the people who ”need to know”. |  |
|  | Always store card holder data, and the machines used to print or copy it, in secure locations, where no unauthorized personnel or visitors are allowed. |  |
|  |  |  |
|  | Distribution. Only distribute cardholder data to other departments and third parties after: |  |
|  | You have approval by management. |  |
|  | Marking the information as ”confidential” and sending it via trackable and secure routes. |  |
|  | Encrypting the data when sending outside the company network. |  |
|  | When working with vendors who provide sevices to store, protect or process cardholder data, always make sure they sign a contract that makes them comply to all DSS requirements. |  |
|  |  |  |
|  | Sevice vendors, like electricians, cleaners and other crew must also be bound in contractual agreement that encompasses all DSS requirements. |  |
|  |  |  |
|  | If a vendor must enter premises storing confidential cardholder data, always make sure they wear the company issued ID badge and are always escorted. |  |
|  |  |  |
|  | Sometimes incidents do happen, and protected information may get stolen, lost or improperly used. |  |
|  | In such cases, always report the incident, no matter how big or small it appears to be. |  |
|  | Incidents include:  Faxing to the wrong number. |  |
|  | Using unsecured networks for sending sensitive information. |  |
|  | Emailing sensitive information to the wrong customer. |  |
|  | Leaving an unlocked an unsecured computer unattended. |  |
|  | Leaving passwords in plain view. |  |
|  | Misplacing documents containing cardholder information. |  |
|  | Our company relies on you to follow all 12 DSS requirements when handling cardholder data. |  |
|  | Now you know why that is important. |  |
|  | Thank you for watching! |  |