According to statistics, employees are the weakest link in an organization in terms of cybersecurity and are often considered the prime cause of data breaches. However, at the same time, employees can be a cybersecurity asset for an organization – provided they have the right knowledge and training to identify and handle the threats.

So what should an effective security awareness training include? When designing a training program, it’s imperative to cover all potential threats your organization faces. In this article, we will outline five important aspects that must be included in a security awareness program.

1. **Phishing Scams**

Phishing scams are the most common method used by cyber criminals to target an organization. Employees regularly get emails, and many of them open them without giving a second thought. Hackers take advantage of this vulnerability and target employees by promising them some fake incentives such as a business opportunity, prize, or free travel, along with creating a sense of urgency.

Hence, every security awareness training must emphasize on identifying and dealing with phishing emails. Examples should be given about common methods used in phishing scams including the following tips:

* Don’t trust unsolicited emails
* Always filter spam
* Don’t send personal or financial information to people who request it via email
* Securely configure your email client
* Don’t click suspicious links in an email from an unknown person
* Be wary of email attachments
* Besides email, also take precautions while handling SMS, social media messages and enterprise collaboration platforms.

1. **Malware**

Malware or malicious software is used very commonly by cybercriminals for stealing sensitive user information such as [cardholder data](http://www.cardzgroup.com/ScratchCard.html) or bank account details, or damage your organization’s system resulting in huge financial losses (ransomware). Malware is delivered in numerous ways including phishing email, removable media or drive-by download.

Security awareness training should cover the malware aspect and include common ways of delivery, threat potential and impact on your data. Along with other detailed information, it must include tips such as:

* Do not install unauthorized software program
* Always keep your antivirus up and running
* Use a firewall at all times
* Don’t download any unknown files through email or websites
* Immediately contact your security team if you suspect a malware infection

1. **Password Security**

Password is the most common method of authenticating a user. Many employees create dozens of accounts online that they can access through a username and password. If password security practices are not followed, they can risk the entire organization’s network. Hence, your training content should include some important password management tips such as:

* Use a different password for every online account.
* Use a password manager that generates and stores unique, strong passwords for every account.
* Generate passwords randomly
* Use multi-factor authentication where possible, to lessen the impact of a compromised password

1. **Removable Media**

Removable storage media is an easy tool for hackers to help them enable malware and bypass network-based security checks of an organization. The malware gets installed through removable media if executed automatically via Autorun or by keeping catchy filenames and tricking employees into clicking the file. This removable media can install ransomware, steal your data or even destroy the computer it is inserted into. Malware infected removable media can come into your employee’s possession at conferences or public events. Hence, they must be trained to manage any second-hand removable device. You should train your employees to:

* Never plug an untrusted device into their computer
* Get all untrusted removable devices scanned from the IT or security department
* Disable Autorun option on all computers.

1. **Privacy and Data Management**

Most of the organizations, especially those dealing with customer data, collect, store and process sensitive information. It includes customer information, business plans, employee data, and other forms of data relevant to the organization. If this data gets exposed to the public, cybercriminal or a competitor, your organization can not only face penalty but also suffer from huge loss to consumer relationships.

Employees should be trained on how they can manage confidential business data and protect their customer privacy and data security. This important training content should include:

* Data classification strategy of the organization and how data can be classified at each information level
* Regulatory requirements affecting routine operations of an employee
* Approved and unapproved locations for storing sensitive data on an enterprise’s network
* Using strong security practices for accounts that hold sensitive data

**Key Takeaways**

Employees are an important asset of every organization and play a vital role in the success of a business. Untrained and unknowledgeable personnel can put an organization at the risk of potential data breaches. Hence, organizations must implement a security program that encompasses all aspects of securing and preventing security incidents resulting from human error.

Besides annual or biannual trainings, it’s also important to give reminders frequently in the form of emails, office posters or flyers. Make training material easily available and provide incentives to employees who take proactive measures in ensuring security within the organization.