REVALSYS
CREATING POSSIBILITIES

HOW TO PREPARE YOUR EMPLOYEES
FOR PHISHING ATTACKS

Article from Revalsys Technologies

This article explains about how to prepare employees for phishing attacks

No matter what the size of your business is, as its owner the security of your data and your employees must be your priority. The internet has changed the way people do business, but it has also exposed companies to cybercrimes. One cybercrime that is carried out using emails is phishing.

The word “phishing” is derived from “fishing”. This is because fraudsters posing as organizations “fish” for user email credentials online and lay out a “bait” in the form of a genuine-looking email. Phishing emails contain malicious links and are usually sent out in bulk with the intent to steal victims’ personal and financial information. Phishing has been around since the ‘90s, but it became widespread after the early 2000s. It is on the rise now with everyone working from home after the outbreak of the ongoing global coronavirus pandemic.

Most employees are unaware of the security threats that companies face, and inadvertently fall for phishing attacks. These attacks can cause a loss of business as well as reputation for companies. However, once your employees gain an understanding of how these attacks happen, they will be able to prevent them easily. Here’s how you can prepare your employees for phishing attacks:

Train Employees To Spot A Suspicious Link

Not many people know of phishing even in today’s digital age, and small businesses assume that they won’t get affected by phishing scams. If your employees don’t know what threats they could be facing, they won’t know what to look out for. Teach them about HTTPS links, the methods used in a phishing attack, and the information attackers look for so that employees know what data they need to protect. Train them to check the email addresses of senders, the formats of emails, and the extensions of attachments. Let employees know that attackers use trending topics and news to target users. For instance, attackers will now pose as health officials and send their victims links claiming to provide COVID-related information.

Inculcate Good Password Habits In Employees

Password security is the foundation of cybersecurity. The most used techniques to secure accounts are using passwords that are combinations of letters, numbers, and special characters, using different passwords for different accounts, and changing passwords frequently. However, using passwords for multiple accounts and changing them repeatedly may cause password fatigue in employees. Passwords are also easy to guess. Get your employees to use two-factor or multifactor authentication. These methods use multiple steps to secure accounts like passwords, OTPs, and biometric authentication methods like facial/finger recognition.

Get Experts To Educate Employees

The advantage of having expert training sessions is that information from experts is credible. Get expert speakers in the area of cybersecurity to educate your employees about phishing risks, the types of phishing attacks, the importance of protecting emails against these attacks, etc.

Conduct Surprise Phishing Attack Tests And Reward Employees Who Fare Well In Them

This is the most important step in the training process and yet one that most companies often skip. You should test your employees after their training to make sure that they are ready to face phishing attacks. Send them a fake phishing email without notifying them. Once employees click on the link in the email, they should be taken to a page that informs them about their mistake. When an employee does well in this test and avoids clicking on the link, remember to reward them. These surprise tests are an opportunity for your employees to learn from their mistakes.

Track The Progress Of Your Phishing Training And Keep Making Improvements

All the employee training sessions and surprise tests that you conduct will help you to know which departments of your organisation are the most susceptible to phishing attacks. Using this information, you can monitor the effectiveness of your phishing training and plan the future sessions as well as strengthen your organisation’s phishing protection.

CONTACTS

For more information on Revalsys Technologies, visit www.revalsys.com

8-2-293/82/1/83-A, 1st Floor,
Road No 12, Banjara Hills,
MLA Colony,
Hyderabad - 500034
Telangana, India

Phone: +91 7032660301

info@revalsys.com