Cisco sends fake phishing emails to employees to teach them not to click miscellaneous

Over the past few years, Steve Martino, information security manager at Cisco has developed smart techniques to fight against cyber attacks.

Earlier this month, one of the three largest US credit rating firms Equifax was attacked by hackers, taking the names and social insurance numbers of about 143 million customers. The case greatly affected Equifax's reputation, heavy stock prices and two senior managers lost their jobs.

Nobody wants to be in a situation like Equifax. The large and small company all adopt the possible measures to protect themselves against cyber attacks. It's not easy, but Cisco's CIO also has its own way.

Cisco employees must always pay attention because Martino always finds their weaknesses, inculcating their heads to protect themselves.

Here are his suggestions to help your organization not become the next victim of cyberattacks.

Ignore click rates

With online business, the click-through rate (Click Through Rate) is very important, indicating that customers click on your link and website to purchase the product.

But in businesses, this high rate is very dangerous because many phishing emails and other tricks are trying to entice employees to click on the poisoned link.

Every quarter, Martino sends fake emails to all employees. Anyone who clicks on the exclusive link will be able to watch videos that teach how to avoid suspicious emails. This way helps employees understand their role in protecting the company before attacking the network.

Property protection

It is difficult to protect yourself against all attack methods, so it is best to focus on protecting the most important data. Martino recommends listing the most sensitive company and customer data as well as the most vulnerable ports.

'If you don't know what matters most and try to protect everything, you probably won't protect anything,' Martino said.

Search for weaknesses

'You have to know that in this world of association, no matter how you do it, there's always a mistake,' Martino said. From employees clicking on fake emails, programmers create error software . people often make mistakes.

Hackers will find errors, so the security team should actively look for available errors. One way is to find network security software and when it finds errors, there is a plan to make things worse.

Practise

Everyone knows the fastest way out of the building in an emergency. The same with dealing with cyberbullying. Martino recommends making a network security guide with specific steps.

Rehearsals are one of the ways to deal with disasters, including network disasters

In particular, everyone has his role and the company should practice rehearsal in case of cyberattacks. The more you practice, the more prepared and prepared you will be when the attack actually takes place.

Information disclosure

The guidebook is very important to the security team in the company, but other departments should also have a plan to deal first, especially the media group.

There should also be a plan to inform the board of directors and shareholders. Don't forget to apologize before the press. 'If there is no feedback manual, you will talk and make many mistakes,' Martino said.