3 Steps to Keep Manufacturing Operations Safe from Phishing Attacks

Verizon reports that phishing attacks remain the number one cause of data breaches, particularly in the manufacturing sector. In just the first half of 2019, more than 4.1 billion records were compromised. Alarmingly, attackers hope to gain trade secrets, compromise personal and financial data or even disrupt manufacturing processes.

Manufacturers can, and should, implement high quality firewalls and automatically scan incoming emails for suspicious attachments or links. But technology cannot eliminate the human factor. As cyber criminals increase the sophistication of their attacks, end users must learn how to recognize and counter phishing attacks when they occur.

Common Phishing Attacks

First, take a minute to understand the most common types of attacks:

- Deceptive phishing – The attacker imitates a legitimate business to steal information. For example, you may receive an email that appears to come from a vendor, asking you to address a problem with your account.
- Spear phishing – As with deceptive phishing, these involve emails from a recognized sender designed to trick the victim into divulging sensitive information. However, spear phishing

attacks use personalization to target specific users. Consequently, they prove far more successful.

- Vishing and SMiShing – Again, attackers mimic legitimate contacts. But in the case of vishing and SMiShing, they contact the victim via phone call or text message.
- Pharming – Some attackers skip the baiting step and focus their attention on directing users to malicious websites. By changing the IP address, they gain the ability to misdirect users to a fake site even when the user enters a legitimate website name.

1. Recognize the Signs of a Phishing Email

Cyber criminals have successfully used many of the same techniques for years. Signs that an email may be part of a phishing attack include a sense of urgency, a generic greeting or subject line, attachments and poor grammar or spelling.

However, as phishing attacks grow in sophistication, it can prove difficult to distinguish a real email from a fake. Remember that a legitimate company will never send you an unsolicited email to request confidential information or money. Nor will they call or text you out of the blue to request that information. The same holds true for government agencies.

Look carefully at the sender's email address. For instance, a business sender typically does not use public internet accounts like Gmail or Yahoo. But keep in mind that fraudsters can spoof email addresses and make an email look quite authentic. As a result, always verify before clicking a link or providing information. And never open an unsolicited attachment.

2. Learn How to Expose Fake Websites

As a first step, before clicking a link, always mouse over the link to see a preview of the URL. Alternatively, type the URL directly into a new window, rather than relying on the link. Some signs of a fake URL include a slightly incorrect company name, "http://" instead of "https://" and extra characters or phrases in the link text.

Fraudsters can spoof websites as easily as they spoof email addresses. And you cannot assume that the locked padlock at the left of the URL guarantees the security of the site. Consequently, you should look for additional red flags like pop-ups that ask you for your credentials. Additionally, look for reliable contact information instead of simply email or a chatbot.

3. Protect Your Organization with Simulations

Training and security awareness campaigns can make a difference in educating end users. In addition, to make sure the lesson sinks in, consider conducting phishing simulations. These simulations involve sending phishing emails periodically to employees and tracking the result.

Start by training users about phishing and providing a method, such as an email address, for employees to report suspicious activity. Then periodically send phishing emails to a few users at a time. Think like a cyber-criminal. Use a sense of urgency, personalization, requests for sensitive information, attached files and so forth.

Track email open rates and click through rates. Then follow up with a general email to indicate that a colleague has reported a phishing attempt. Use the email as a teaching tool by highlighting the red flags. Additionally, follow up with further training as necessary.

Take Control of Cyber-Security

You have heard the bad news. Cyber-crime continues to rise, costing manufacturers millions of dollars. But keep in mind the good news that you can take control of your cyber-security. Address the human element with training and simulations. At the same time, engage a security expert to help you develop a comprehensive cyber-security strategy.

The security professionals at eMazzanti provide security consultation and a full suite of world class services to keep your data and your business safe. From cloud security to encryption and network monitoring, we have you covered.