6 Email Security Tips to Defend Against Increasing Attacks

Know what to look for and arm your organization with six simple, but effective, defense strategies.

Email is Weapon of Choice

Cyber criminals stole more than $3 billion over the last three years through Business Email Compromise (BEC) scams. Those scams targeted small and mid-size businesses (SMBs), in particular. According to the recently published Internet Security Threat Report (ISTR) from Symantec, email has emerged as the weapon of choice for cyber-attacks in 2016. Sadly, while one in 220 emails contained malware in 2015, that rate increased to one in 131 emails in 2016.

Attackers now favor spear-phishing email campaigns that target specific individuals, organizations or businesses. The highest rate of phishing emerged in companies with between 251 and 500 employees. With now professionalized spamming operations, malware authors often outsource their spam campaigns to highly organized groups.

Election Tactics

Cyber criminals use several general tactics to spread malware and ransomware. A favorite method involves disguising malicious emails as routine correspondence, as we saw in the 2016 U.S. presidential election.

In March 2016, an email that appeared to originate from an official Gmail account was delivered to the account of Hillary Clinton's campaign chairman, John Podesta. The email suggested that his account had been compromised and instructed him to reset his password. As we now know, the victim unknowingly clicked a malicious URL and delivered the password to the attackers.

Social Engineering

Most businesses receive thousands of emails each day. With increasingly sophisticated and targeted attacks, it can prove difficult to recognize malicious emails. More and more often, cleverly disguised emails use social engineering, relying on human interaction to trick users into breaking security protocols.

Increased email security is necessary to help businesses guard against common social engineering tactics, such as:

- Use of financial keywords in subject headings (terms such as Invoice, Order, Payment or Bill)
- Emails that appear to come from a scanner, printer or other similar device (keywords such as Document, Scan, Fax)
- Email delivery failure message that contains malicious spam (keywords like Mail Delivery Failure)

Anatomy of Email Infection

Emailed malware typically follows this basic process:

1. A malicious email enters the system disguised as a routine message. For instance, the subject may suggest that the email contains an invoice for recently purchased goods. The email address, text and attached documents may appear genuine at first glance.
2. The email contains an attachment. Most often, that will be a JavaScript file (a .wsf file) or a Microsoft Office file.
3. When the victim clicks on the attachment, the file executes a PowerShell script that downloads the malware. Often, the downloaded malware involves ransomware, blocking access to systems or files until a ransom is paid.

6 Critical Email Security Tips

Savvy users have already adopted simple email security measures such as immediately deleting vague emails and not clicking on attachments unless they come from a trusted source. As attackers employ greater sophistication, businesses need to build more sophisticated defenses.

Some basic, but powerful, email security measures you may not have implemented:

- Ensure that your business email system includes a multi-layered, proactive security solution. Also, keep security and operating system software up-to-date.
- Enforce a robust password policy to ensure that employees use strong passwords and change them regularly.
- Use extreme caution with any Microsoft Office email attachment that instructs you to enable macros to see its content. Use similar caution with JavaScript or .wsf attachments. Unless you can verify the source, immediately delete the email without enabling macros.
- Establish clear procedures for communication of sensitive information. Be wary of any email that suggests a departure from normal security protocol.
- Instead of simply clicking "Reply," obtain the supposed sender's email address from a corporate address book and send a reply to that address.
- Before clicking a link in an email, be sure that the link is legitimate. For example, type the URL directly into the address bar, or hover your cursor over the link to display the full URL.

Multi-faceted Approach

Now more than ever, email represents a prime source of disruption and loss for businesses. By taking proper security measures, you can protect vital data and systems from attack. First and foremost, know what to look for. Then, build and communicate modern security protocols throughout your organization.

Most importantly, invest in multi-layer email security. A comprehensive security system is critical to protecting your business from malicious cyber-attack. With commercial-grade security equipment and automatic updates to guard against the latest threats, you gain both peace of mind and enhanced productivity.