FBI Tech Tuesday: Building a Digital Defense with an Email Fortress

Businesses Beware—Fraudsters want to cash in on digital data, and your vulnerable e-mail account can give them the keys to the kingdom. One of the biggest dangers lurking in your in-box is a version of a phishing scheme.

In this case, the fraudster sends you what appears to be a legitimate e-mail. He may have hacked someone else’s e-mail account to get to you, or he may have “spoofed” an e-mail address making it look real.

Either way, his goal is to get you to give him access to your company and/or your cash. In this phishing scheme, an embedded link is the hook with which he will attempt to catch you.

Once you click on that link, the fraudster is able to download malware onto your system that potentially gives him access to user ID’s, passwords, customer records, financial information, and data files.

Phishing schemes are often just the start -- leading to potential ransomware attacks, business-e-mail-compromise scams, and more.

So -- how do you protect your company? From the lowest level employee up to the CEO, your e-mail system needs to be a fortress filled with defenses.

- Don't use free web-based e-mail accounts for your business. Establish your own domain and create e-mail accounts based on that domain.
- Ensure that your firewalls, virus software, and spam filters are robust and up-to-date.
- Immediately report and delete suspicious e-mails, particularly those that come from people you don't know.
- If you receive an e-mail from someone who appears to be a legitimate contact; but you are wary, make sure you “forward” it back to the sender. Do not hit “reply.” That way you can manually type the known e-mail address or find it in your established contact list to confirm authenticity.
- Don't click in a moment of panic. Fraudsters often use social engineering to stress you out so you will act quickly without thinking. Check before you click.
- Consider two-factor authentication for employee e-mail. This would include something you know (such as a password) and something you have (such as dynamic/changing PIN or code.)
- Create a security system that flags e-mails with similar -- but incorrect -- formatting. For instance, you may regularly do business with Joe at ABC_company.com, but are you going to notice if one day the e-mail comes from Joe at ABC-company.com?
- Make sure your e-mail is encrypted in-transit if you are putting sensitive information into it.

Bottom line -- build the e-mail fortress tall and wide to protect your business. For more information on e-mail security concerns or other cyber crimes, check out the FBI’s website at www.fbi.gov or the FBI’s Internet Crime Complaint Center at www.ic3.gov.

FBI Portland, Beth Anne Steele, May 30, 2017
https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/fbi-tech-tuesday-building-a-digital-defense-with-an-email-fortress