Five ways to make your email safer in case of a hack attack

December 19 2014, byTami Abdollah

The Sony hack, the latest in a wave of company security breaches, exposed months of employee emails. Other hacks have given attackers access to sensitive information about a company and its customers, such as credit-card numbers and email addresses. One way hackers can sneak into a company is by sending fake emails with malicious links to employee inboxes. Here are five simple steps to make your email more secure and limit the harm a hacker can have:

ARCHIVE EARLY AND OFTEN

Most corporate email systems allow people to set up regularly scheduled archiving so that emails are moved off of the server after a certain number of days. You can still check archived emails on your work computer, but they are no longer easily accessible on websites outside the office or on your phone. That limits hackers' ability to access those emails too. You can make exceptions for emails that you want to keep in your active inbox, and they won't be archived.

GET ORGANIZED

As emails come into your inbox, deal with them. Sort them into folders. This segments your data, requiring an attacker to know which folder to go to, or to take multiple steps to search for wanted information. Paired with archiving, it also ensures that what the hacker does compromise is limited and known for any future damage assessment. Sensitive information can also be removed from your inbox. For example, delete an email and save what you need to your hard drive or an external drive.

KEEP WORK AND PERSONAL EMAILS SEPARATE

Don't use your work email for personal email or activities online. That limits details a hacker can glean about you to conduct more sophisticated attacks targeting you as the entryway into your company's system. For example, hackers can learn about your shopping habits or personal hobbies and use those to send a phishing email that appears to come from websites you bought goods from or read frequently. Phishing messages route you to a fake address and allow hackers to gain access to your system.

DON'T CLICK ON UNEXPECTED LINKS AND ATTACHMENTS

If you receive an email with a link or attachment you weren't expecting, send the person a separate email asking whether the first email was legitimate. For links from companies such as banking institutions, hover your cursor over the hyperlink or right-click to show the link's final destination. Before you click, make sure the address that pops up when you hover over the link matches where the hyperlink says you'll be sent. If unsure, use a new window and physically type in the website's address to conduct your business.

IF YOU SEE SOMETHING, SAY SOMETHING

If your email is acting up or a link or attachment strikes you as strange, forward it to your IT department as quickly as possible. Your attention and fast response may prevent someone else at your company from making a mistake.

Citation: Five ways to make your email safer in case of a hack attack (2014, December 19) retrieved 24 April 2024 from https://phys.org/news/2014-12-ways-email-safer-case-hack.html