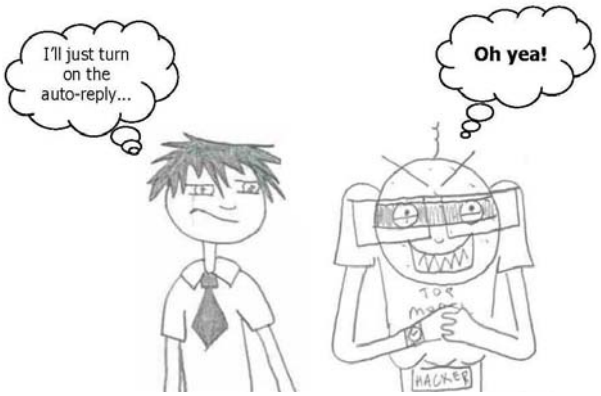
Auto-Reply Basics



Technology. It's here and people are not afraid to use it. They want to take full advantage of its possibilities. No stone left unturned so to speak. This includes an e-mail system's Auto-reply feature. When we are out of the office, we don't want our clients or other business associates to sit and wonder why we are not responding to their e-mails. We want them to be aware that, for the time being, we are out of the office and will get back with them when we return.

But almost every new technology introduces us to new vulnerabilities. E-mail is no exception. Beware that "black hat" attackers wreaking havoc with phishing attacks will not go away after multi-factor authentication is fully implemented. These attackers will use anything they can to gather information that can be used against an individual or business, and implement what is called an orchestrated attack. By combining seemingly innocent requests for information and other information gathering methods, these criminals can compromise a financial institution's system. This includes information given out with a user's Auto-reply feature.

Thus the purpose of this article: Be careful! When using your e-mail's auto-reply feature, you need to be selective in what you divulge. Many attackers send out a rash of e-mails, just waiting for a recipient's auto-reply to kick back a response. From there, these crafty individuals will use what information they get to plan a phishing attack or perform pre-text calling, gleaning information that can be used against you in the process. Any bit of information they get can be used in the larger picture of identity theft or masquerading.

In addition, spam attacks can gain momentum with auto-reply messages. Attackers use the messages to enter an endless look of auto-replies replying to auto-replies. This, in the long run, can result in a denial of service, loading mail servers with users' auto-reply messages. In addition, they can be used to send viruses or worms to innocent victims.

The easiest way to mitigate risk with a particular technology is simply to cease using it. From a policy perspective, consider discouraging or even prohibiting the use of the auto-reply feature altogether. But if you must use your e-mail system's auto-reply feature, here are a few tips to keep things under control and to be a little safer:

- DO keep messages simple. State that you are out of the office, but don't state your reason for being gone.
- DO get permission before divulging an alternate contact's information.
- DO be careful about what you state about your job title (the higher up the ladder, the more attackers attempt to gather and use information).
- DON'T be specific about the dates you will be away from the office.
- DON'T divulge an associate's e-mail address (this is more fuel for their fire). Give a phone number of someone that can help them in your absence instead.
- DON'T divulge personal information in your auto-reply message (home phone, cell phone, etc.).
- DON'T set auto-reply messages for your home e-mail. (You may get a very unwanted visitor while you are gone!)

Another step that can be done (see your network administrator) is to use your e-mail system's filter settings. It's simple to filter out e-mails that contain auto-reply words or phases in the subject line or header. You can have these messages directed to your "trash bin" rather than having them inundate your "in" basket. This is useful for those loops that the attackers may have set up.

The bottom line is: be careful when using your system's auto-reply feature. You never know who will be the recipient! And as always, if your company allows auto-reply, be sure to increase user awareness about the vulnerabilities.

About the Author:

Bobbette Fagel, CISA, CISM
Vice President
infotex, Inc.

Bobbette is a Certified Information Systems Auditor and Certified Information Security Manager, and has worked with Infotex since its inception. She has been intimately involved in compliance projects for financial organizations and hospitals, and leads our efforts on compliance program development as well as policy and procedure. She handles the reporting aspects of Vulnerability Assessments, Network Architecture Reviews, IT Audits, etc. She has a great understanding of the FFIEC guidelines and stays on top of changes in those guidelines. Bobbette helps clients understand the metrics of risk analysis as well as the business case for information security expenditures (and more importantly, the risk acceptance case for NOT making those expenditures).