Today's INSURANCE PROFESSIONALS®

Fall 2016 Volume 73 Issue 3

REIMAGINING RETIREMENT

Do You Have a COOKIE-CUTTER *Retirement Plan?*

TECHNOLOGY TRENDS SHAPING INSURANCE *IN* 2016

THE GREAT GENERATIONAL SHIFT

10 Common Security Mistakes That Can Hurt Your Network

by: Jerry Fetty, CEO

No insurance employee intends to become a security risk, but the digital world is complicated, with deviously packaged threats around every corner and malicious programs just waiting for a rushed and unwary end-user to slip up. The recent widespread attack on Office 365 corporate users with zero-day ransomware virus underscores the need for diligence at your organization. Here are 10 common security mistakes to avoid:

1. **Ransomware Emails –** One of your HR employees checks her email and finds what looks like a job application directed specifically to her, using her name, title, and other personal identifiers. Unaware that the email came from a hacker who did a bit of research on Facebook and LinkedIn, she clicks on a link and downloads a slew of viruses. A particularly nasty form of this fraud is ransomware. Once it is downloaded, it causes a Windows error, which on reboot, locks the user out and demands a payment for a decryption key to regain access. Employees should not download any attachments from an unfamiliar source or any that are not relevant to them based on their job function (i.e. invoices, sales inquiries, etc.).

2. **Lax Habits in Mobile Security –** You may have the latest versions of spyware and anti-virus software on your company desktops, but do your employees have the same on their tablets, phones, and other portable electronics? Without the same security, these devices, when connected to your network, can leave you wide open for breaches. Be sure your employees aren't leaving points of access to your network without safeguards by establishing mobile device policies and a BYOD (Bring Your Own Device) policy.

3. **Weak or Personal Passwords –** As much as your employees might love their dogs, cars, or a particular date in time, a password is no place to express that love. Also, if they actually use "password" as their password, they are inviting trouble. They should use private, randomized strings of numbers and letters for their passwords.

4. **Clicking on Risky Websites –** We've all done it. Spent far more time than we thought we would to search for something on the Internet. So when we finally find a promising link, we tend to not think about the source. As a result, that link could bring you to a site to download malware, exposing your network and files to any number of threats. Configure your browser to always ask before running files and downloading automatically.

5. **Using Unsecured Connections to Access Sensitive Data –** Are your employees reviewing company files during their lunch break using a local restaurant's free Wi-Fi? If they are, you should put a stop to it; public Wi-Fi hotspots are a popular avenue for hackers and malware to access devices.

6. **Lost or Stolen Unencrypted Tech –** An employee is riding the bus to work, and leaves a company phone behind on the seat. Without encryption software, that phone is potentially an encyclopedia of company data and information for sale to competitors, as well as a free pass into company files and email. Enforcing encryption policies helps to mitigate this risk.

7. **Shadow IT –** An employee decides she prefers a different program to perform a job-related task and downloads a copy of that program onto her company desktop without the knowledge of the IT department. The program spreads your company data into yet another system, but this time you don't have control over it. Plus, there is always the risk that the download will come with an unwanted bonus -- vulnerabilities that could allow malware to hitch a free ride into the network. Your company needs to be vigilant regarding the use of unapproved, personally downloaded applications.

8. **Personal Email Use –** Using a personal email account for work purposes is never a good idea. Beyond the implicit unprofessionalism of some usernames, personal accounts tend to be more vulnerable to malicious programs than their corporate counterparts. Encourage your employees to keep work and personal emails separate.

9. **Leaving Workstations Unattended –** As unfortunate as it is, not all employees will be on the up-and-up. Some will attempt to view information they aren't cleared to access, often for purposes of corporate espionage. This task becomes remarkably easy when a workstation is left unattended while still active. The fix is relatively easy to establish: just remind employees to log off of their desktop (or at least lock it) before they leave their post, and enforce this policy.

10. **Using Random Memory Devices –** It makes no sense to carefully craft your system defense if your employees have no qualms about plugging a random USB drive they found lying on the street into their workstation, subjecting your network and files to whatever malware might be on the device's storage.

While human error is impossible to avoid entirely, you can minimize your risk of a security breach by implementing these policies for your organization's employees.

About the Author

Jerry Fetty is founder and CEO of SMART I.T. Services, Inc., an Information Technology service company that specializes in helping independent insurance agencies increase their productivity and profitability by harnessing the power of technology. He also served as a Board Member for the MSP Alliance, the world's largest professional association and accrediting body for the Managed Services Industry. He can be reached at (586) 258-0650 or jerry.fetty@smartservices.com.