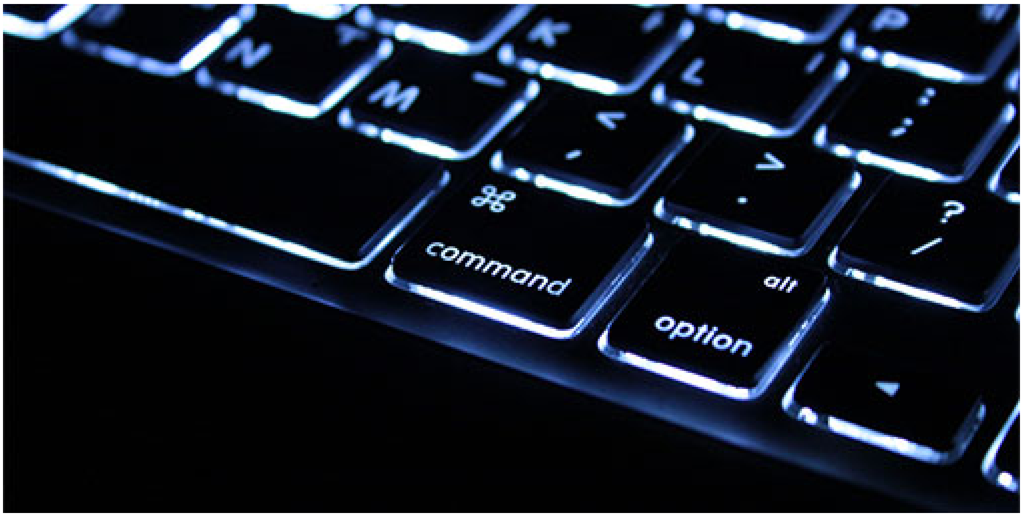
CARLTON FIELDS

9 Things Employees Should Do to Prevent Data Breaches

September 15, 2015

Co-Authored by Gary Slinger, Manager of IS Process & Security



Businesses are facing increased financial burdens due to the rise in data breaches caused by malicious and criminal attacks. In addition to the obvious costs incurred to detect and fix the effects of a breach, lost business is potentially the most severe consequence. And lost business can translate into lost jobs. It is often said that it takes a village to defend against cyberattacks. Employees of every organization must realize that they are members of that village, and need to do their part to protect their employer. Avoiding employee mistakes that lead to inadvertent failures will free up valuable resources to fight the bad guys—and may save your job.

> *The sooner an incident response starts, the greater the chance of managing the incident successfully and minimizing any damage...*

Employees should adopt the following "safe" practices to minimize their mistakes and help thwart criminals: **1. Avoid Password Re-Use**

- Use a different password for each system you access, and make it secure and complex—for example, don't just increase a numeric value as you change systems.
- Use a password manager (for example, LastPass, 1Password, or KeePass) to manage your passwords, and ensure you use a complex passphrase for the password manager.

- Specifically, don’t use your work username/password combination for personal systems.

User awareness of the dangers of password re-use has evolved. For instance a 2003 report indicated 65 percent of users used the same password for different applications or services. By 2013, that figure reportedly fell to 55 percent. Password re-use is one of the single biggest threats to account security if two-factor authentication is not used. Consider the recent Ashley Madison data breach that allowed more than 11 million username and password combinations to be released into the wild. The threat, if those passwords and usernames were also used to access those users’ email, bank, or other system accounts, is obvious and far exceeds exposure and embarrassment. The 2015 Verizon Data Breach Report, as quoted in an IT industry blog, said “… we find that most of the attacks make use of stolen credentials…” and “Over 95% of these incidents involve harvesting creds [sic] from customer devices, then logging in to web applications with them.” **2. Where Possible, Use Multi-Factor Authentication** Your employer may require this for your corporate systems, but increasingly it is also available for personal systems. Google Two-Step Verification is available for Android and Apple phones/tablets, and provides two-factor authentication to Google applications. For instance, increasingly, work and personal matters intermingle in electronic messages and documents. Multi-factor authentication provides another barrier against having one username and password provide access to multiple systems. **3. Don’t Click That Link!** Your bank will never email you a link that asks you to enter your name, social security number, and password into a form full of spelling mistakes. These requests are as suspect as pleas from Nigerian princes. In 2015, phishing, spear phishing, and ransomware attacks have been prevalent across all types of businesses and companies. Some look more real than ever. Instead of following emailed instructions to call or click, you should generally go directly to your bank’s website or call from a number you have (perhaps found on the back of a credit or debit card). Phishing and spear phishing are used to collect data or propagate malware. **4. Change Your Passwords Regularly** Even with two-factor authentication, passwords remain the first line of defense. Use your password manager, and change your passwords every 90 days. Some password managers will automate this for you, going through all your saved sites and changing the current complex password to a new one, and storing that information for you in the password manager database. Why does this matter? Let’s consider the Ashley Madison breach again—the username and password combinations are available. The passwords are encrypted, but given enough time and computer power, they will be decrypted (more than 11 million have been so far, as noted earlier). If you use a complex password and change it regularly, you will ideally be using a new password by the time a breach occurs and your old password is broken. **5. Practice Safe Wi-Fi** If you use a computer, cellphone, or tablet on a public Wi-Fi, are you secure? Usually, perhaps. But cheap technology exists to create fake Wi-Fi hotspots that capture your network traffic, usernames, and passwords. Consider investing in a personal VPN, or ask your IS/IT department about access to a corporate one. This tool will encrypt your network traffic at its source, before pushing it out over an unencrypted, and potentially compromised, public Wi-Fi network. This guidance applies at coffee shops, train stations, airports, shopping malls, and anywhere else with “free” Wi-Fi. In these places, think carefully about transmitting a username and password without additional protection. **6. Keep Your Devices Close and Consider Their Contents** If you lose a cellphone, do you have the ability to wipe its contents? What if its data is compromised before you can do that? Always know the location of your phone, tablet, computer, etc. Know whether you've set up "Find My iPhone"—or a similar remote location tracking app or service—and how to use it. Your company may be able to lock or wipe your phone as well, you'll have to ask. Similarly, while you probably do need to have all of your company contact details on your phone, consider whether you really need complete copies of all your corporate data. Perhaps you only need the information you're currently working on. Consider using secure cloud storage services, or keeping your data on corporate servers, and accessing it remotely, rather than downloading it locally. **7. Patch Baby, Patch!** Your company is (hopefully) patching your computer regularly—you should do the same for your home computer(s)—and also do software updates for your cellphones and tablets. Undisclosed and uncorrected computer application vulnerabilities are an ever-present threat, and may involve additional patches out of sequence to the usual patch release cycle. This kind of threat is usually well publicized across the web. Turning on automatic updates and/or notifications on your computer and other devices may also help. **8. Remember the Physical World!** Walking away from your computer to get a cup of coffee? Lock the screen. Put a lock code on your cell phone. Don't leave devices unattended in public spaces—you risk their physical theft, and exposing sensitive company information. Bank statements? Credit card bills? Utility bills? If you're not keeping them, don't just throw them away, shred them. At your office, don't throw away anything that includes company information, such as sales figures, contact information, and marketing plans. Shredding should be your default option. Harvesting information from improperly disposed of paper is one form of information gathering used for identity theft or systems breaching. **9. Notify Early** If you think a breach or other failure has occurred, talk to somebody, such as your computer security officer or CIO, or call your bank's fraud hotline. The sooner an incident response starts, the greater the chance of managing the incident successfully and minimizing any damage. The Verizon DBIR mentioned earlier also notes that attackers who get into a system can be there for up to 205 days on average before their presence is known. That number can be brought down through vigilance and reporting anything that appears unusual. Perhaps your user account was locked out when you got to work today. It may, or may not, mean something. So, talk to your security team. We all love being able to access the Internet during the work day. But as attacks continue and losses increase, employers may be forced to limit such access in ways that most employees will find inconvenient. Therefore, employees should take seriously the importance of their efforts in "cyberhygiene." *This originally appeared as a JD Supra Perspective on September 15, 2015.*

Related Practices

Business Transactions
Cybersecurity and Privacy
Labor & Employment
Technology

Related Industries

Technology

Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.