5 Ways to Know if You Are a Data Security Risk

By John Kogan

When we help law firms implement security programs, we take the expected technical measures: we plug up holes in the network, apply encryption where necessary, install monitoring solutions, and so on.

But the most important aspect of any security program, user training and awareness, is also the one that is hardest to control with any degree of certainty. Because it's not the tech that's putting your firm most at risk—it's you.

If you study trends among data breaches, you will notice that human error causes a large proportion. This is not to say you should feel bad about yourself and your trusting nature. Scammers and hackers are scarily smooth these days (it's not for no reason that 2018 is being referred to as the year of the scam[1]).

Here are some way to know if you are putting your client's data at risk.

1. YOU ARE QUICK TO CLICK ON HYPERLINKS.

Avoid clicking on links in emails, especially if they are from an unknown sender or sent without context. A good way to verify links before clicking is to hover your mouse over them. Do they lead where they purport to? Check carefully for tricky typos like "arnazon.com."

If you do click on a link, never enter sensitive information into the window that opens.

2. YOU WANT TO BE EXTRA HELPFUL BY EMAIL AND ON THE PHONE.

Say you get an email from a partner of your firm: they are stranded abroad, have lost their wallet, and need your help immediately. It's natural that your first instinct would be to help, but think twice.

Even if the email does seem to be from someone you know, be on guard if it seems out of character. Watch out for odd spelling and grammar, threats of negative consequences, and requests for fund transfers. If it seems weird, it probably is.

By extension, be careful when someone calls you requesting information about you or a colleague.[2] These kinds of scams are called social engineering, and they are remarkably effective.

3. YOU LOSE YOUR GADGETS AND DON'T DISPOSE OF THEM PROPERLY.[3]

Are you the type to leave your cellphone and credit card behind at restaurants, or forget your laptop in a cab? I can relate.

Aside from causing headaches, such slip-ups can also lead to major breaches if your lost items end up in ill-meaning hands.

To avoid worst case scenarios, make sure everything is encrypted and, at the least, password-protected. Your phone should have a pin or a forensic safeguard, such as fingerprint scanning or facial recognition. Your laptop should be encrypted with a solution such as Microsoft Windows's BitLocker.

4. YOU USE THE SAME PASSWORD FOR EVERYTHING.

I know, it's become so difficult to remember all our passwords. Still, do try to avoid repeating them, and definitely, do not write them on a post-it note that you stick to your computer monitor. If one of your accounts is breached, the rest of your accounts with the same password will be at risk as well.

We recommend using a password manager such as Roboform, which creates complex and unique passwords and remembers them for you. Browsers such as Google Chrome are also starting to offer complex password management now.

John Kogan, Chief Information Security Officer at Kraft Kennedy, is the Director of Managed Services, with a special focus on cybersecurity. His team provides ongoing support, monitoring, and technology planning to organizations. He has an extensive background in IT and business developed over 35 years of working in financial services, consulting, and Fortune 100 corporations.

Also, consider multifactor authentication. If someone does get a hold of your password and tries to enter it on an unfamiliar computer, they will not be able to log in without a second verifying step, such as a prompt on your cell phone.

5. YOU HAVE LOCAL ADMINISTRATOR RIGHTS ON YOUR COMPUTER.

This is common at small firms. Having administrator rights means that you are able to make big changes on your work computer, such as installing new programs. While it may be convenient, it is also dangerous, as it makes it easy for malware and hackers to access your firm's core systems. Your IT department or provider should be the only one with administrator privileges.

1. Will Yakowicz, *The 3 Biggest Phishing Scams of 2018*, Inc.com, July 6, 2018, https://www.inc.com/will-yakowicz/biggest-email-phishing-scams-2018.html.

2. *A Hacker Shows How You Can Take Over Someone's Online Account in Minutes Using Nothing But a Phone*, Business Insider, Feb. 25, 2016, https://www.businessinsider.com/hacker-social-engineer-2016-2.

3. *Security Alert: BleedingBit Affects Cisco, Meraki, Aruba Access Points*, Kraft Kennedy, Nov. 14, 2018, https://www.kraftkennedy.com/security-alert-bleedingbit-affects-cisco-meraki-aruba-access-points/.