SANDBERG PHOENIX

PROFESSIONAL LIABILITY BLOG

Professionals Beware — Strong, Unique Passwords Reduce the Risk of Liability

AUTHOR: ZACHARY MERKLE

Professionals have access to sensitive data. Accountants need financial and tax records. Health professionals routinely handle protected medical information. Real estate brokers and title companies deal in large financial transactions with financial information and wire instructions. Lawyers need access to all of the above, depending on the context.

Now think of all the passwords a typical professional has — one password for email; another for the business computer; maybe a different one for a document management system or cloud storage account. There are passwords for bank accounts, other financial institutions, secure emails, client portals. A typical individual has tens or hundreds of passwords between personal and professional accounts.

Ask yourself: are all of those passwords different? Do you use *MydogLucy5!* for multiple accounts, say your email with EmailProvider(dot)com, your client trust account at BigBank, and your social media account at SocialMediaSite(dot)com? As a professional, access to highly sensitive data means strong passwords are essential.

Because one of the most common data breaches happens like this (simplifying to make my point): a hacker breaches one company's system and obtains user names and passwords for all that company's users. Then, hackers transport the username-and-passwords combinations just discovered, trying them on other websites. So, if your login credentials on SocialMediaSite(dot)com get compromised, and you've got the same password for your client trust account at BigBank and your work email at EmailProvider(dot)com, you are at risk. Your client data could be compromised, and you and your firm could be liable.

What is the solution? Creating strong passwords that are different for every website or login in your life. That way, hackers cannot transport passwords from one data breach to other websites and services. And, with strong passwords, hackers cannot simply guess your password by, say, inputting some variant of Wikipedia's Most Common Passwords.

But how, you might ask, can I remember all of those unique, strong passwords? One solution is a password manager. A password manager stores, in an encrypted database, all of your passwords so that it is possible to use unique passwords on every site. That way, you can focus on remembering one very-strong password, which encrypts your password manager's database (and, of course, is used nowhere else). Other common features of modern password managers include suggested strong passwords, auto-filling passwords, and notifications when a particular website is hacked (so you can change your password immediately). While this blog doesn't endorse a particular product, there are many reputable password managers out there, and many reputable publications to guide you — see, for example, a recent article from Wired, The Best Password Managers to Secure Your Digital Life.

Cyber threats are among the most important areas of exposure for professionals. And unfortunately there is no way to completely eliminate the risk. But improving password habits — strong, unique passwords for every login — is a worthwhile way to reduce that risk. Check out password managers to help you out.