The Freelancer's Guide to Cybersecurity Podcast Episode 10: Zombie Accounts Are Killing Your Cybersecurity

Episode released 12/10/2020

Transcript

Today, the topic is zombie accounts, those accounts that keep on keepin' on long after you've forgotten them. Problem is, they haven't forgotten you.

Your zombie accounts are likely more of a threat to your cybersecurity than the apps you use every day! Here's why and what you can do to protect yourself from the undead.

Why are zombie accounts such a threat to your security? The short answer is that every account you have—whether you use it often or never—has the potential for being breached, exposing you to a range of threats, from theft of your credentials (meaning, your login username and password) to fraud and identity theft.

Your continued accrual of accounts—for everything from a login you created to shop at a website just once to portal logins you have for professional organizations or even trial accounts for an app or magazine—this slow incremental buildup increases your digital footprint.

Your digital footprint—all of this information about you available online, including these one-off accounts you have forgotten—this footprint makes you vulnerable, and the larger it is, the greater the likelihood your data will be exposed in a breach. Each of these breaches, no matter how minor—well, each breach increases the number of data points about you that are available to bad actors, who are pretty good at connecting the dots to create a complete picture of you.

Zombie accounts—those online accounts you create but never close, say for a fitness device you got rid of years ago, or that one-time shopping experience on a website—these accounts languish unattended, their passwords unchanged and potential problems left unnoticed by their owners. Kind of a situation of out of sight, out of mind. The number of zombie accounts you have likely grows each week, each month, each year, and each one of these zombie accounts is another potential data point for a hacker's file.

And no, these accounts don't need to have credit card information or other sensitive data to be dangerous to you. Whether it's a social media account you accessed via an app on mobile device, like a cell phone or tablet, or an online banking account that you used to process payment from a client back in the day, they all have information about you a hacker can use to threaten your security and privacy.

Some cyberspace risks are beyond your control, but, be that as it may, many cyberspace vulnerabilities absolutely are under your control.

First, it's important to take all of this personally. Realize that you and your business are a target. So many people think that, because they are not a millionaire or a celebrity, they are not big or important enough to be a target. And, in a way they are right: Their business and individual assets may be negligible and not worth a hacker's time if you still picture hackers as disaffected types living in their parents' basement.

But that's not the business model for cybercrime in the 21st century. The cybercrime of today is big business, and it's a serious threat to individuals and small businesses.

As a small business, you are more likely to be seen as a conduit into the systems of companies you contract for because you are likely a pretty weak link in that supply chain. Larger companies have gotten much better at cybersecurity and vetting their contractors. It's the smaller companies, subcontractors, and the independent professionals who work with them that don't have cybersecurity support—and are more vulnerable to attack.

It's also important to realize that much of this cybercrime that will affect you personally or your small business is automated. Spearphishing, the very individualized, specific attacks on the big fish, like millionaires and celebrities, can require a lot of effort, and it's a high-risk enterprise. But gathering up a large school of small fry like you and me in an automated net requires a negligible expenditure of money or effort precisely because it can be done with bots and algorithms, and it results in a big profit. Catching a bunch of fish in a net is a pretty low risk enterprise. According to ThreatPost, account takeover attacks—attacks that use data gleaned from breaches and then is aggregated—"cost consumers and e-commerce retailers $16.9 billion in losses."

So what can the average independent professional do to safeguard their professional and personal data and privacy?

This time I will start with what NOT to do. Do not load up on a VPN with dark web capability and go spelunking on the darknet looking for what information of yours is on it: this is way out of your league. Know your speed and stay in your lane, which, if you listen to this podcast, is most likely the Clearnet—that is, not the dark web. In the show notes you will find a link to a Clearnet source you can safely use to find a list of what breached data of yours has been published on the darknet.

With that information in hand, address what you find there by, first, securing any breached accounts. Some breached businesses and institutions offer identity theft monitoring services to affected individuals, but usually only when substantive sensitive data, like social security numbers, were breached. You may choose to take them up on that offer.

Then decrease your risk moving forward by shrinking your digital footprint, that is, killing off your zombie accounts. Determine which accounts you no longer use and delete them. AccountKiller.com gives guidance for closing accounts at popular sites, and some software, like Dashlane, will assist you in the process if you find it daunting. Links to those and other resources can be found in the detailed show notes.

Then follow some good basic cybersecurity hygiene. Change your passwords regularly, using unique and secure passwords or passphrases. Use only secure connections and minimize your footprint by using a secure browser and search engine combination, like the Mozilla Firefox browser with DuckDuckGo search engine.

In doing so, you will minimize the vulnerabilities discussed above and decrease the amount of “curation” you need to do to keep your online life secure and private.