# The Freelancer’s Guide to Cybersecurity Podcast Episode 3: Have You Been Pwned?

Episode released 10/07/2020.

Transcript

What do hackers know about you (and your small business)? How do you discover what they know about you, and how can you protect yourself (and your business) moving forward?

On today’s episode we ask, “Have you been pwned?” More likely than not, yes you have, which means information about you is available on the dark web. What’s the dark web? It’s where data—from passwords to social security numbers and credit card information—is bought and sold, fueling cybercrime. It’s the big data for what has become a big business.

Today I’ll share why being pwned is a problem and how you can safely discover what the dark web knows about you. Then of course we finish with easy and inexpensive ways you can minimize the harm done and learn from the experience to safeguard yourself—and your business—from future cybersecurity threats.

Unfortunately, we hear about site breaches all the time. The usual advice is to change your password on that site. Obviously, changing your password to a site that you know has been breached can go a long way to safeguarding your cybersecurity . . . on that site. But that breach, even if hackers only got your login information, is just a small part of a much larger problem. Because, consider this: Hackers aggregate breached data, and every bit of data about you, no matter how small, from each breach helps hackers create a more complete profile of you.

All this information, when aggregated, is your digital footprint.

Like a mosaic–in which separate, individual tiles have little value but when used together form a complete picture–these individual bits of breached data may have limited value when considered separately, but, when taken together, create a complete profile of you and therefore pose a very real threat to your cybersecurity, enabling everything from identity theft to account takeover attacks.

And when your data is breached from online accounts and corporate databases and made available to bad actors (hackers) . . . you’ve been pwned.

For everyone without a video gamer in the household, “pwned” means “owned,” meaning soundly beaten. Thumped. Thrashed. In the cybersecurity sense, if your login credentials or sensitive information like your social security number, work history, date of birth, etc. has been breached and now resides on the dark web, accessible to hackers and other bad actors, you have indeed been pwned.

You may ask yourself why this is a problem if your login credentials were stolen—you can just change your password, right? Or even, who cares who knows about my work history—anyone on LinkedIn knows that in a general sense. The fact is, most folks understand why getting specific sensitive data like their social security number put up on the dark web opens up issues of identity theft and fraud. A stolen social security number can be used to open up a credit account in the victim’s name, saddle them with debt, and ruin their credit rating—making getting any sort of loan for a car, a house, or even another credit card nearly impossible. But, while obviously very important, your social security number is not the only piece of data you need to worry about.

Because people tend to use the same password across multiple accounts, hackers can use that password to access other online accounts you might have. This is called credential stuffing—using that username/password combination on other sites—and it’s incredibly effective because credential stuffing is automated. The automation of the credential-stuffing process allows hackers to efficiently test your password—and variations of it and other information they have gleaned about you on the dark web and the Clearnet—on thousands of websites in mere minutes. In other words, if a site is breached and your login data stolen, the odds are quite high other accounts of yours will be compromised.  When credential stuffing works and accounts are successfully compromised, or hacked, it’s called an account takeover. This is why cybersecurity specialists advise people to not use the same password for multiple sites.

Look, it’s no surprise that many people believe their information is secure with the companies they trust, but this couldn’t be further from the truth. For example, the job and career site Monster.com’s user data was exposed, but they didn’t tell anyone because it happened through a third party, which is a sad excuse to sidestep responsibility and loss of reputation. My point is, if you assume all entities you deal with report their breaches as required by law and basic ethics—that’s naïve.

Another consideration is the data about you being warehoused, traded, and sold by companies you never directly engaged with, so, even if you heard of a breach of their systems, you would be totally unaware of the threat to your own security. Ever heard of popular data conglomerate Verifications.io? They are an email validation service. Well, you may not have heard of them, but they’ve likely heard of you and 2 billion more of us, and they have our data, as do hackers now that Verifications.io has been breached. As CEO of nCipher Security, Cindy Provin, summed it up for *Digital Journal*:

“A leak of 763 million* records is massive. Not only were emails publicly accessible for anyone with an internet connection, but phone numbers, birth dates, mortgage amounts, interest rates and social media accounts were also exposed.”

*It’s now known it was 2 billion records. Either way, it’s a big number. For reference, the population of the United States is estimated at about 330 million.

Big numbers get tossed around. So yes, absolutely—if you think you are too small a target for a hacker to sit around inputting your username and password into sites until they get a hit, you’re absolutely right. But you’re *not* too small a target for them to get your data as part of a large database that they feed into an algorithm that does all the work for them.

And that’s where your problem begins. Depending on the sites that can be accessed through credential stuffing, hackers can access extremely sensitive information about you, such as your credit card information, work history, or social security number, which could lead to identity theft.

You also need to consider that the fallout might not be restricted to your personal identity. What business or client accounts can be accessed with your credentials? As large businesses get better at hardening their systems against cyberattack, hackers are using the credentials of contractors and subcontractors to access those systems directly or through parallel systems. Increasingly, contractors and their subcontractors are the weakest links in business’ cybersecurity.

Small businesses—including every 1099 independent professional–have become lucrative cyber targets for hackers, fraudsters, and bad actors since mid-size and large businesses began getting their cybersecurity act together a few years ago. And yet, too often I hear from my small-business colleagues, “I’m too small to be of interest to a hacker.” It’s simply not true.

Phishing and business email compromise (BEC) attacks account for a lot of the fraud perpetrated against small businesses, and they get a lot of press. But it’s worth remembering that many small-business owners use tools meant for home use, leaving their data vulnerable. Consider that each antivirus software package for the home use market is estimated to catch only 2/3 of extant threats—which may be fine for home computers used to write reports for school, emails to friends or do a little bit of e-retail therapy—but it doesn’t stand up to the rigors of constant use and screening of files coming in from multiple sources around the globe. And even the mundane personal account can pose a threat to your business security: the breach of a business owner’s personal fitness account that results in stolen credentials may result in the hack of that business owner’s cloud storage or bookkeeping app on which s/he stores customer and client data.

It’s really just that simple.

*So now* are you convinced that this is A Thing? Want to know not if but what data of yours has been breached and can be found on the dark web? Well sit down, take a deep breath, then visit ';–have i been pwned? The link is in our show notes. And don't worry, the site is safe—it's the go-to site for this sort of information on the Clearnet, meaning the safe part of the internet.

The site, also referred to as HIBP, lists data breaches in which your data has been involved and is floating around the dark side of cyberspace. You may already know of some of the breaches, like the breach of customers' sensitive financial data by the credit rating giant Equifax. Other breaches may have happened without your knowledge of your data's involvement–like Verifications.io.

It may be a bit of a shock to see all the accounts from which your data has been breached, but realize that denial of the problem is not an existential threat to the problem itself. After you've taken it all in, be proactive in protecting your cybersecurity moving forward.

So let's get to the point…now that you've seen what information of yours has been breached and is available online to any sort of bad actor, the question is: What can you do?

Well, the bad news is: you can't un-ring a bell–the information about you that has been hacked is out there and persistent.

What you can do is safeguard your privacy moving forward and *limit your digital footprint.* These 5 easy steps will get you started.

1. If you haven't already, change your password on each of the breached accounts. Practice good password hygiene (different passwords for every site; each at least 8 characters long; each a mixture of digits, special characters, upper and lowercase letters; password changed frequently). Avoid using names, birth dates, etc, of family members and pets—that information is likely found online and in social media accounts—if not your accounts, accounts of family members and friends. Also, avoid using words found in the dictionary. The oldest form of cyberattack is the brute force attack, which uses words found in the dictionary to crack passwords. It's still used decades after its first use because it still works.
2. Change the credentials for every site on which you used that credential (username + password) or a version of it (different username but same password or same username with similar password). Optimally, refresh your passwords on all your online accounts using the guidelines for good password hygiene in #1.
3. Close accounts you don't use. These are called zombie accounts. And you can become very vulnerable through these accounts precisely because you are not monitoring them. They can be breached and either taken over or the information in them used to create, again, this big data set that we're talking

about. Yet another data point that can help hackers take over your accounts or threaten your cybersecurity in another way.

4. Note what other data has been stolen, then decide to limit the data set you will willingly share with random sites and Facebook “quizzes” moving forward. Your date of birth, your first pet’s name, the city in which you met your spouse—just stop! Those are common security questions for online accounts, so keep these things, as much as possible, private.
5. Sign up for data breach alerts. Mozilla Firefox Monitor will automatically alert you when you appear in HIBP.

Proactively safeguarding your digital life is not hard, it just requires knowing where to look for threats, what tools to use, and a willingness to apply these tools consistently.

Until next week, stay safe.