DT The Distribution Team

We wrote THE BOOK on Distribution Inventory Management

Stay Safe Online: Tips to Avoid Getting Hacked

By Jason Bader

As with most of my articles, the content or theme comes from personal experiences. This month is no exception. Recently, my LinkedIn account was hacked. I received this email from LinkedIn stating that an additional email address had been added to my account. I then received a second email stating that there had been some suspicious activity and did I make these changes. By the time I read these emails and attempted to log in, some bad actor had changed the primary email to their own, wiped out my login credentials and essentially took over my account. I experienced the entire range of emotions – fear, anger, self-pity, and finally acceptance. LinkedIn is one of my primary marketing vehicles for podcasts and other services. The thought of rebuilding my 3000 plus connections and profile was not something I was looking forward to.

Fortunately, after 10 very frustrating days, I was able to find a contact in the LinkedIn security department (big shout out to Andrew Chung) who helped me clear out this basement-dwelling squatter and restore control of my account. Not only was this a tremendous relief, but it has sent me on a quest to plug the leaks in my online boat. Nothing like a swift kick to the teeth to shift one from reactive to proactive mode. Since this incident, I have done a bit of research on how to mitigate this type of invasion in the future. Here are some of the challenges and solutions that made the most sense to me.

Password Negligence

I am truly guilty of this. I have used the same passwords for so many of my online accounts without regard for the sensitivity of the product. My financial services, travel, and my shopping accounts used the same passwords. My social media accounts often had the same passwords as well. In hindsight, this was simply foolish. It was like having the same key to my home, vehicles, office, and safe deposit box. As an alternative, my research suggested the use of password management software that will randomly generate a very strong set of random characters whenever you open a new account somewhere. The program then stores this information and uses auto-fill technology to log you into the account. This is one of the areas where autofill is positive, I will talk about the negative aspects later.

As an additional measure, I would encourage you to turn on something called Multi-Factor Authentication (MFA) whenever possible. This is becoming more prevalent in the online world. Essentially, when the service doesn’t recognize where you are entering from (either browser or IP address), a verification code is sent to either your phone or email. This is the second layer of protection even if your login and password information has fallen into the wrong hands.

Network Security

Like many of you, I travel extensively and often find myself taking advantage of free WIFI opportunities in hotels, airports, and coffee shops. While these opportunities are certainly welcome where mobile service is limited, they do come with certain potential risks. When we jump on an unsecured network, even if there is an access password, there is a chance that someone is “listening in” to our digital stream. They could be gathering information on sites that we visit and ultimately capture our credentials. Conversely, there have been incidents where malicious software has been delivered to unsuspecting users who tap into the unsecured WIFI stream.

Using your own mobile hotspot to provide a connection for your other devices is one way to get a tighter handle on your digital connections. Most smart phones have this feature and date usage limits seem to be plentiful. Another security solution is to use Virtual Private Network (VPN) software to secure your online connection. These services create an encrypted connection so that eavesdroppers can’t follow you around looking for site credentials or secure information. These services are inexpensive and should be part of any traveler’s arsenal.

Auto-Fill Convenience

If you are anything like me, online shopping has become a way of life. If I haven’t visited the UPS store to pick up packages in a couple of days, they call my cell to check if I’m OK. Being one who believes in working smarter, not harder, I tend to take advantage of shortcuts in all aspects of my life. Shopping is no exception. Over the years, I have allowed Google to store and fill in my address information to facilitate a quicker shopping experience. Furthermore, I have also had Google store credit card information to speed up the process. Google Pay and Apple Pay may feel like a wonderful convenience; but these services, as secure as they may seem to be, leave us a bit vulnerable. Just be careful that we are limiting the auto-fill usage to reputable sites and use other security measures, such as fingerprint or facial recognition, to authenticate the process.

Social Media Sharing

For me, this is where this whole mess started. I post information on LinkedIn. I use it to share my podcast episodes, comment on other’s postings, and generally let my thoughts be known in a limited way. I try to avoid too much personal sharing as I believe that this is a business platform. On the other hand, I have been dragged into the more personal side of social media using platforms like Meta and Instagram lately. I am certainly not a super user of these mediums; but who doesn’t like a scrolling dopamine hit every once in a while?

There are certainly many cases of personal attacks and manipulations though these platforms, but I wanted to key in on one that has always made me a little more cautious. Travel related posting can be fun in a “my life is better than yours” kind of way. Sorry. My Gen X cynic was feeling left out of the conversation. Unfortunately, there are dangers in sharing when you are away from your home. In a 2011 study by researchers at the University of Florida found that approximately 78 percent of ex-cons surveyed admitted that social media played a role in their selection of homes to target for burglary and other property crimes. These participants noted that vacation-related posts were key factors in their process.

Furthermore, social media profiles and posts can give important information to con-artists and online scammers. Clever criminals can dupe friends and relatives into giving up sensitive information by posing as close friends who know details about your life, such as your place of work, restaurants you frequent, your travel plans, and even your personal relationships.

My intent is not to scare anyone here. I am simply sharing what happened to me and how it has helped change my thinking around the subject of cyber security. I am by no means an expert. If you want a greater understanding of how your person and business assets can be compromised, I encourage you to seek out a professional on the subject. I interviewed an expert a few years ago on my podcast and I would be happy to pass along his information. Before I let you go, I would be remiss if I didn't urge you to back up your data. As I was reeling with the thought of having to rebuild my LinkedIn network, I was cursing myself for not backing up my connections. When was the last time you backed up your critical contacts, emails, and work documents? Be smart, be safe, and know that I am always here to help.

About the Author:
Jason Bader is the principal of The Distribution Team. He is a holistic distribution advisor who is passionate about helping business owners solve challenges, generate wealth, and achieve personal goals. He can be found speaking at several industry events throughout the year, providing executive coaching services to private clients and letting his thoughts be known in an industry publication or two. Lat year, he launched his first podcast, Distribution Talk. Episodes can be found at www.distributiontalk.com and most podcast applications. He can be reached at (503) 282-2333 or via email at jason@distributionteam.com. You can find additional resources on his website: www.thedistributionteam.com