brandprotect™

September 2015 | Briefing 9

LEARNING FROM ASHLEY MADISON

EVERYTHING YOU DO IS FOREVER.

It's happened. A breach that people really care about. The Ashley Madison breach, and the subsequent public pillorying of those who were caught with their virtual pants down, has driven home two of the most fundamental challenges of living in the digital age.

In these executive threat briefs, BrandProtect has tried to give you insights into the ways that cyber criminals think, and how common cyber scams work. You've written to us that this is great information, and you have shared it widely across your organization. But have you changed your own personal behavior? Because underlying all of those ThreatBriefs rests the same truth. Your online choices matter. They will follow you for a very long time. **In this month's brief, we will try to bust some of the most common myths that many of us rely on when we are online.**

1) I'M NOT A TARGET.

In today's fast-moving online world, we are all targets. Think for a moment about your personal devices. Do you use them at home and at work? If so, they cross over your company's traditional security perimeter. When you are outside your company's security perimeter, you are still part of your company's attack surface. If a criminal compromises your device, or gains access to your email, or learns one of your passwords, they will try to parlay that incursion into something that has much more value – access to a financial account, or a corporate network, or access to your home.

2) I DON'T REALLY DO MUCH ONLINE.

Think about this – how does a mapping application know where there is traffic ahead? Do well intentioned citizens call them up and report on local conditions? No. The mapping vendors have access to millions of real-time location sensors. In fact, probably one or two in every vehicle. Your phone. Even when you are not using your phone, it is broadcasting your location constantly. The mapping company pays to have access to this movement data, which they can manipulate into surprisingly accurate traffic flow reports. This is just one example, The kind of location tracking that is a staple of modern spy films, is mostly fact-based. When you carry a phone, you are actually online all the time. And when you are online, lots of information about you is online too.

YOU ARE YOUR OWN WORST ENEMY.

3) I USE A STRONG PASSWORD.

Yes. Please, use the strongest passwords that you can. Use two-factor authentication whenever possible. Install a password manager to increase the complexity and the diversity of your passwords. But don't think that your strong passwords will always shield your data from prying eyes.

4) I'VE "LOCKED DOWN" MY PRIVACY SETTINGS.

It would be great if it was that easy. Or that permanent. Facebook is often called out here, because of the massive amount of very personal information that their users willingly post and upload, but the truth of the matter is that most online services are constantly tinkering with their privacy policies. What's private today may be public tomorrow. And you won't really be able to do anything about it. Just assume that everything you put up online is public, or will be public someday.

5) I CAN DELETE THAT.

No. You can't. It is astonishingly hard to make things disappear from the Internet. And this goes way beyond the "right to be forgotten". Services are implemented with fail-over redundancy, data centers are co-located (at least) and information is constantly backed up using methodologies that are amazing. The costs of keeping historical information have plummeted. So what do you think happens? The historical information gets saved. Those photos you posted on Facebook back in 2005? They are still there. The caustic tweets you sent when you were a young, opinionated professional? They are somewhere. That email you drafted and never sent? It's somewhere too…

6) THE CREDIT CARD COMPANY WILL KEEP MY INFORMATION SECURE.

While that is the idea, how has that been working lately? Stolen credit card data is widely available on the Internet – advertised through forums like PasteBin or through dark web marketplaces. With credit card data, the criminals are just a hop step and jump away from knowing where you shop and what you buy. Probably a better assumption would be that your entire transaction history will someday be available for inspection.

WHAT'S OUT THERE, REALLY?

At the requests of a client, BrandProtect is often asked to prepare an Internet Risk Assessment for one of their executives. The results are amazing. Using publicly accessible tools (plus a few special BrandProtect techniques) we are able to gather tons of data about our subjects. Everything from residence and contact information, employment history, education history, home ownership history, family relationships, credit status, club and association memberships, friends and family, vacation spots, employment history, and much more is unearthed. The resulting reports are many pages long, and serve as a cautionary tale for our clients.

ONLY DO THINGS THAT WOULD MAKE YOUR MAMA PROUD.

7) NOBODY WILL TAKE THE TIME TO CONNECT THE DOTS.

Several years ago, a team of enterprising MIT students (very smart people) built a tool that parsed what people posted on Facebook, the groups they joined, where they posted, who their friends were, what their friends posted, etc. They were able to learn a lot about the network of people they studied, just from their public posts. In this era of big data, and massive data availability, connecting the dots has never been easier.

8) I'M VERY CAREFUL.

No matter your personal discipline, you are constantly being dragged online by the actions of others. You are tagged, CC'ed, mentioned, and approached in posts, photo uploads, emails, videos, association member lists or worse, phone lists.

So, at the end of the day, how can someone be expected to stay safe in this dangerous world. It is really very simple. Only do things that would make your mama proud.

brandprotect™

www.brandprotect.com
sales@brandprotect.com | 1.866.721.3725

For enterprises concerned about their business exposure to increasing online risk, BrandProtect™ provides a complete suite of world class Internet threat detection services to monitor the entire social Internet spectrum and mitigate business risk arising from fraudulent or unauthorized online activity. BrandProtect helps security, risk management, and marketing organizations at leading financial services institutions, large-scale retailers, insurance providers, telecoms, pharmaceuticals and more, protect their brand value and business bottom line.