October 2014

Cybersecurity: Halting Hackers

Rachel Vipond

Iowa State University

Follow this and additional works at: http://lib.dr.iastate.edu/ethos

Recommended Citation

Available at: http://lib.dr.iastate.edu/ethos/vol2015/iss1/15

This Article is brought to you for free and open access by the Student Publications at Iowa State University Digital Repository. It has been accepted for inclusion in Ethos by an authorized editor of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.
If you don’t have a fingerprint scanner on your phone, you probably have a passcode or pattern enabled. Text message verifications now flood in when you log into banking apps, and you’ve been told that using the same password for every thing is bad. Maybe this password is your pet’s name or you’re one of those using “password,” which has consistently been listed as the most widely used password on the internet. Whether it is poor password choices or weak security on sites you visit, something has to be done to combat threats to your personal data. Cybersecurity is the word on everyone’s lips, but what exactly is it and what does it do?

A broader term for cybersecurity is “information assurance,” explains Professor Doug Jacobson of the ISU Information Assurance Center and on faculty for electrical and computer engineering. This gets to the heart of what cybersecurity is all about—protecting your data. Referring to the CIA model of confidentiality, Jacobson explained that cybersecurity means more than just keeping your credit card numbers away from hackers. It aims to maintain your information as it fits your needs—maintaining the integrity of your information, keeping it available to you when you need it, or confidential when it is for your eyes only.

It’s likely you’ve caught a headline or two about the nude celebrity photos that were leaked from their iCloud accounts recently. Sparking scandal and talk of lawsuits, it’s no wonder that cybersecurity is a hot topic.

Iowa State has taken note of the demand for better cybersecurity. In fact, Senator Chuck Grassley spoke at Iowa State earlier this year on the topic, and the university has received $2.38 million to promote cybersecurity. Cyber-defense competitions are put on across the country, with students and amateurs doing their best to break through firewalls or resist attacks. So, what does all this hype mean for the average Blackboard-using, smartphone-addicted, Facebook-browsing college student? As it turns out, a lot.

If you use Facebook, online banking, heck, if you’re a student at Iowa State, you have personal data online. Cybersecurity is what keeps that data in the place you want it, and away from those who would exploit it.

“People approach the computer as a harmless device, an inanimate object that can’t hurt [them]... but it does provide direct access to people who do want to hurt [them],” says Jacobson.

A reason cybersecurity is more important now than ever is that hackers can make money off their exploits.

“The hackers used to be in it for the thrill of the game, but now it’s a huge criminal enterprise,” explains Jacobson.

Once your data is stolen, they set up websites to sell it to the highest bidder.
To address this problem, certain institutions are stepping up to educate and make people more “security literate.”

“To sit there and tell somebody to make a good password doesn’t really tell them anything. Unless they know why—what a password [does] for me and what does it not—these lists of things for them to do [to be more secure] have no context,” Jacobson says.

Iowa State is meeting these literacy needs with classes and education efforts. In fact, any student can take COMP E 131, a course in cybersecurity.

The government is making an effort to teach the public as well: the “Stop. Think. Connect.” educational campaign aims to teach public about cybersecurity threats and what they should do to protect themselves through simple modules on a website.

Back to those fingerprint scanners. Have you noticed that your passcode is generally required in addition to your fingerprint scan when you first turn on your phone? This is called multifactor authentication, and you use it every time something requires an email or text confirmation, or you trigger a security question. These have been met with some resistance because they require an extra step and therefore more time. That being said, extra time shouldn’t keep you from embracing multifactor authentication—passwords by themselves just aren’t that secure. Coupling the password with another form of proof that it’s you unlocking your iPhone? Much more secure.

“There is a tradeoff between security and convenience,” explains Jacobson, “but it’s inconvenient to unlock your house—it’s inconvenient to push the buttons to your apartment.”

Some apps, like 1Password, attempt to make multifactor authentication a little simpler. 1Password creates strong passwords for sites that it encrypts and stores, controlled by a master password that you create as well as biometric data. Its design allows for higher security with fewer steps.

Security is often either hyped up to the point of paranoia—think that uncle who forwards you chain emails about internet conspiracy theories—or ignored almost completely (have you used the same password for everything since MySpace was still a thing?). The key to keeping a level head is knowing some of the basics. For instance, it’s important to know that personal computers are by default what Jacobson refers to as “exit only doors.” This means that bugs and viruses will attack your computer only if you let them in. If you’re not running a server (and you likely aren’t), you have the ultimate say in what comes into your computer. Knowing this, it makes sense that you should be choosy with the websites you visit, the email attachments you open and the software you download. If they’re from reputable sources, you’re probably safe.

Security technology can be alienating and confusing, but breaking it down can make cybersecurity useful and achieve its purpose: protecting you.

To recap the benefits of cybersecurity, Jacobson offered five tips to the average student to improve their security. If you change anything about your habits, make it these:

1. Run a firewall on your computer, and antivirus or malware software. As to which brand is best, Jacobson says, “They’re all the same. Pick one, run something.”

2. Be leery. Though in general Midwesterners tend to be quite trusting, this shouldn’t carry over to their computer use. Always look at your credit card or debit card transactions for oddities. Small, $0.89 iTunes purchases and other “micro-transactions” are a way hackers check to see if they can get away with bigger purchases. If your information has been stolen and you don’t catch these, chances are that the account-draining purchases will come only a day or so after the small ones. Because of this, Jacobson mentioned that credit cards could offer more security than debit cards because they actively monitor purchases for odd purchase locations or unusually high purchases.

3. Be careful when sharing passwords with others—or don’t do it at all. This is especially true for sharing within relationships—what if it goes sour and they’re holding a grudge?

4. Change your passwords often. “I always tell people: when you change your Facebook status, change your password,” says Jacobson. Even if it’s something as mundane as a Facebook account or an email account, being hacked can do a lot of damage.