Is Hacking the New Normal?

By Judge Herbert B. Dixon Jr. (Ret.)

It seems that I am writing a lot these days about privacy and hacking. Last spring, I wrote an article entitled "Is Your Internet Device Spying on You?"[1] Later, I wrote a slightly different article entitled "The Wonderful and Scary Internet of Things!"[2] Now, I approach the subject again, asking, "Is Hacking the New Normal?"[3] I guess you might say I have become fixated on the idea that malicious hacking events are eroding expectations of privacy. Are these hacking incidents occurring a little too frequently? Below are some examples of recent events and a few final thoughts about cyber protection.

Malicious Toys

As the 2017 Christmas season approached, I saw warnings about toys with microphones, cameras, and recording capabilities that may spy on children.[4] Much of the data collected by these devices is stored in the cloud. If these devices were the subject of hacking, private information might be accessed by unauthorized persons if, for example, the child responded to questions from the toy such as "where do you go to school?" "where do you live?" and "what time do you go home?" This is not a new issue arising just before the 2017 Christmas season. Indeed, in July 2017, the Federal Bureau of Investigation issued a warning to consumers that Internet-connected toys could present privacy and contact concerns for children. The notice included safety recommendations, such as only connect and use toys in environments with trusted and secured Wi-Fi Internet access; understand and implement the toy's Internet and device connection security measures (authentication when pairing the device with Bluetooth using a PIN code or password); install software and firmware patches and updates; and know and understand if user data are stored with the company, third-party services, or both—and whether any publicly available reporting exists on their cybersecurity reputation. These recommendations and many others are important for a child's parent or guardian to know to avoid ugly situations where the child's toy is the enemy or facilitates dangerous situations.[5]

Belated Reports and Discovery of Major Hacking Incidents

Just before Thanksgiving 2017, news reports indicated that Uber was the victim of a hacking incident that occurred one year earlier. The hackers stole data involving 57 million people consisting of Uber customers and drivers. Even more distressing, in what some security experts categorize as an improper effort by Uber to avoid embarrassing publicity, the company paid the cybercriminals $100,000 to destroy the stolen data and keep quiet about this exploitation of Uber's IT infrastructure.

Within days of the news of Uber's hacking, Imgur, a popular meme site, reported a newly discovered three-year-old security breach that affected 1.7 million accounts, consisting of emails and passwords. At this point, I lost my composure. Incidents like these are especially troubling because the only sin by the victimized individual was patronizing an online business to obtain a legitimate service. Have we gone from "Let the buyer beware" to "Let the user beware"?

The biggest known hacking incident of 2017 (as of the time this article was submitted to print) was reported in September 2017. The breach involved Equifax, a global information solutions company, and affected at least 143 million U.S. consumers. Of note, the breach occurred in May 2017—four months before the company reported it. To gain a sense of proportion, the number of U.S. consumers affected by this Equifax breach nearly equaled one-half of the entire country's population. Reports about the breach indicate that names, Social Security numbers, birthdates, and addresses were compromised for most of the affected consumers, and the breach also included credit card numbers and personal identifying information of at least several hundred thousand of these consumers. It appears the hackers gained access to the consumer information by exploiting a software vulnerability, which would have been secured if a patch issued in March 2017 had been installed before the May hacking incident.

In September 2016, Yahoo announced two breaches that earn Yahoo the title "Mother of All Hacking Victims," an honor it still retained when this article went to print. Yahoo announced that data associated with at least 500 million accounts had been stolen two years earlier in 2014. Three months later, Yahoo reported a three-year-old hacking incident in 2013 in which it estimated that 1 billion accounts were affected. Now, after further investigation, Yahoo states all 3 billion of its customer accounts were likely compromised by the 2013 incident, including Yahoo email, Tumblr, Fantasy, and Flickr.

As this article was going to print, the 3 billion accounts compromised in Yahoo's 2013 hacking makes that incident the biggest data breach in the history of the Internet.

Other Massive and Unique Hacking Incidents

Another hacking scenario that caught my attention involved cybercriminals

preying on distracted drivers at gas station locations. As the scam goes, the hackers attempt to access drivers' personal information using Bluetooth technology enticing the distracted driver, who is filling his gas tank, to join a network that pops up on his smartphone screen. This type of incident is a great example of why you should change your default password or PIN to something other than 1234 or 0000.[6]

For additional background, consider revisiting a previous article, "Technological Advancements Coexisting with Tech Stagnation."[7] This article discusses reports on hacking episodes involving JP Morgan Chase and Sony Pictures Entertainment. The massive hack on JP Morgan compromised large volumes of checking, savings, and other bank account data, which security experts said would have been substantially less severe had a network server been upgraded and a routine security fix implemented. In Sony's situation, the hacking incident paralyzed its business operations for several days and included theft of email and employee information. Several security experts, surprised at the extent of the access hackers gained, gave their opinions that the adverse impact of the hack would have been substantially lessened by an active protocol of prevention, detection, and response—prevention to make targeted attacks harder; detection to spot the attackers; and response to minimize the damage, restore security, and manage fallout.

Yes, Hacking Is the New Normal

Is hacking the new normal? Yes, at least for now. Digital transmission and receipt of information and storage in the cloud are now our way of life. Unless and until technology brings us new types of communications methods, there often will be opportunities that provide insecure access points for cybercriminals who want our private data and digital possessions. It is up to each one of us to do our part to secure our digital possessions and information, just as we put physical locks on our other worldly possessions.

As stated by one security professional, there is a multiplier effect as the number of major breaches of consumer data rises.[8] For example, if a crafty hacker gains access to multiple sets of stolen data that include names, mother's maiden names, Social Security numbers from one set, and names and birthdays from another set, that could be a powerful combination of information with which the cybercriminal can contact banks, posing as banking customers, and gain access to accounts. Also, consider a phishing technique where your email account is compromised and someone you know well receives an email from you (not the real you, but your email account) and the email has a malicious attachment that provides a gateway for the hacker into your system. Or because people reuse passwords or make slight variations of the same password, consider how this additional intelligence about you might be just enough to assist a cyber thief in hacking your account.

Conclusion

So, how do we survive the new normal? Below are a few basic cyber protection guidelines for businesses, government entities, and individuals. I have spoken with several cybersecurity professionals about these guidelines. In every instance, they say following these minimum guidelines would significantly reduce or minimize successful hacking incidents. Although the list could be longer and each guideline could be the subject of a separate article, I kept the number of guidelines at 10 because this seems to be an ideal number for a list of commandments to establish acceptable conduct.

1. Become knowledgeable about cyber threats, especially phishing attacks;
2. Be careful about joining public Wi-Fi networks;
3. Update firmware and software;
4. Install patches to resolve known security vulnerabilities;
5. Use strong passwords;
6. Don't use similar passwords across your various accounts;
7. Establish and follow IT protocols;
8. Change the default settings of your electronic devices;
9. Follow and enforce password policies; and
10. Regularly back up your digital data (including smartphones, tablets, computers, and other electronic devices). ■

Endnotes

1. Herbert B. Dixon Jr., *Is Your Internet Device Spying on You?*, 56 Judges' J., no. 2, Spring 2017.

2. Herbert B. Dixon Jr., *The Wonderful and Scary Internet of Things!*, 56 Judges' J., no. 3, Summer 2017.

3. Long after I adopted this title, and as I was finalizing this column, I found an article with a similar name, "Hacking Is the New Normal," in which the author vents about the government's inadequate cybersecurity efforts. Jared Keller, *Hacking Is the New Normal*, Pac. Standard (June 8, 2015), https://goo.gl/fDQSmp.

4. Megan Cloherty, *Hackable Holidays: Dangers of Toys That Spy on Kids*, WTOP.com (Nov. 26, 2017), https://goo.gl/vn3UqD.

5. Public Service Announcement, Fed. Bureau of Investigation, Alert Number I-071717(Revised), Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children (July 17, 2017), https://goo.gl/Ra4bFa.

6. Megan Cloherty, *Hackable Holidays: Bluetooth Scam Hits Drivers at Area Gas Stations*, WTOP.com (Nov. 30, 2017), https://goo.gl/riHTGW.

7. Herbert B. Dixon Jr., *Technological Advancements Coexisting with Tech Stagnation*, 54 Judges' J., no. 1, Winter 2015.

8. Markus Jakobsson, *The Cumulative Effect of Major Breaches: The Collective Risk of Yahoo & Equifax*, SecurityWeek (Dec. 7, 2017), https://goo.gl/ySNAVZ.

Judge Herbert B. Dixon Jr. has retired from the Superior Court of the District of Columbia after 30 years of service. He is chair of the ABA Standing Committee on the American Judicial System and a member of the Techshow Planning Board. He is a former member of the ABA Board of Governors and a former chair of the National Conference of State Trial Judges. He can be reached at Jhbdixon@gmail.com. Follow Judge Dixon on Twitter @Jhbdixon.