Cybersecurity Awareness Month 2022: Updating Software

October 17, 2022
By: Michael Ogata
https://www.nist.gov/blogs/cybersecurity-insights/cybersecurity-awareness-month-2022-updating-software

Cybersecurity Awareness Month is flying by, and today's blog identifies different security vulnerabilities that can be exposed if you are unable to keep up with your software updates. We interviewed NIST's Michael Ogata, a computer scientist in the Applied Cybersecurity Division, and he walked us through different strategies to minimize your cybersecurity risks. Michael also was able to provide cyber tips to improve online safety.

This week's Cybersecurity Awareness Month theme is updating software. How does your work/specialty area at NIST tie into this behavior?

Today, mobile applications are the beachhead of most people's day-to-day interaction with information technology. E-commerce, social interaction, and media consumption are driven via our mobile devices. However, the scope of what can affect the safety of your data reaches far beyond what runs locally on your device. Mobile apps, websites, and online services are connected to a panoply of systems that are often distributed amongst multiple owners. Due to the complexity of all this software, some security vulnerabilities will inevitably be discovered after release to the general public. Therefore, understanding how this software can be more securely designed, examined for vulnerabilities, and better delivered to consumers is paramount. Our work both seeks to improve the state of the art with respect to building better software, but also empowers consumers to make better decisions when selecting and using software.

What is the easiest way to stay safe online?

As we stated above, many vulnerabilities will be identified *after* a user has started using a piece of software. This means the benefits of our work cannot be fully leveraged by consumers unless they understand the importance of keeping software up to date. Many bugs are publicly known and can be exploited by attackers, so if you don't update, you are vulnerable. Sadly, many people don't update their software because of various

inconvenience—but having software with known vulnerabilities is a high price to pay. If your system is online, we recommend keeping up with the updates!

What are three things you can do to minimize cybersecurity risks to a person or businesses?

The importance of this cannot be overstated. Modern and mainstream mobile devices are pre-configured, or can be configured, to automatically update their operating systems and the apps installed on them. Likewise for desktops and laptops. Make sure you have your devices set to do so! However, most, if not all, devices have a finite lifespan after which they will/can no longer receive security updates. Understanding these limitations, and retiring unsupported devices when able, can help to minimize risk. Finally, many consumers neglect applying security updates to the single most important part of their home network: their router. Your home router is the first line of defense against threats that originate from outside your home. Making sure it stays up to date is vital to minimizing risk!

A second strategy you can use to minimize your cybersecurity risk is the use of multi-factor authentication. Multi-factor authentication can help minimize your risk when using online services by placing roadblocks in front of attackers should your password become compromised. If a service supports multi-factor authentication, users should enable it. If a service doesn't, users should be vocal in their requests for that feature or seek alternative providers (especially for services that handle sensitive personal, financial, or medical data). At the minimum, users should look for multi-step authentication mechanisms from their online service providers.

Finally, backing up your data can also minimize the impact of a vulnerability on your personal data. The rise of ransomware has rendered many unsuspecting user's personal files inaccessible. Think about having two kinds of backups – one that is easy to make so you make backups often, and one that will last a long time for data you want to archive – like your family photos. *See our NIST media longevity table for more information.*

What does #BeCyberSmart mean to you?

#BeCyberSmart means understanding how your everyday decisions affect your cybersecurity safety. Every app you install, every site you visit, and every account you create has implications concerning your personal data and safety. Being security aware is a lot of work, but it may pay off by making you less vulnerable. Be selective about the personal information you share on social networks and the accuracy of the content you consume. We at NIST need to #BeCyberSmart by improving the state of the art to help lessen this burden on users.

ABOUT THE AUTHOR

Michael Ogata is a computer scientist in the Applied Cybersecurity Division. Over his 18-year career at NIST he has worked on digital forensics, healthcare standards, mobile application security, cybersecurity for public safety, and cybersecurity for the smart grid. Michael loves science fiction and proudly calls himself a Star Wars fan AND a Trekkie.