Crossing the Digital Divide (v99)

"This, too"

By Joseph Feigon

For the Observer

Lions, Tigers and Bears, oh my. You've heard me stress the importance of updates; Microsoft, Apple, and Android are used by billions of people across the planet. Security flaws may compromise your security, your wallet, and your ID. Keeping devices up-to-date is on-going, not a one-time thing.

This week's column is another author's reminder to safeguard your privacy and the security of your devices, your router should be updated, and in many cases, if a ten+ year old device, replaced. Tercius Bufute provided the following article to Consumer Reports. Good work, Tercius!

Generally speaking, the most interaction people have with their router is the occasional turn-it-on-and-off-again when a slowdown occurs. This benign neglect, however, could be putting their data and even their bank accounts at risk. It's important to regularly update router firmware to keep the security features up to date.

"All of your information is going to be passing through that router," says Craig Young, a researcher with the digital security company Tripwire. "So if it's compromised, it can really impact your privacy and the security of your devices."
Young has some serious router-hacking cred, having identified and responsibly disclosed dozens of vulnerabilities in products from manufacturers such as Amazon, Apple, and Google.

He says router owners face several threats from hackers.

In October, for example, a pair of university researchers discovered a vulnerability that could allow attackers to access usernames, passwords, credit card details, emails, and more flowing through an encrypted WiFi network.

Routers can also be taken over for criminal activities such as illegal downloads and attacks on websites. In 2016, the Remaiten Worm, or KTN-Remastered, spread to numerous Linux-based routers by connecting to random IP addresses and trying out commonly used log-in credentials. Once it gained entry to routers, they were used in distributed denial of service (or DDoS) attacks on commercial websites.

The Problem with Firmware Updates

Router manufacturers typically roll out software updates throughout the year to address such vulnerabilities. In fact, Tejas Shah, Netgear's chief information officer, says his company released nearly 200 fixes for its line of routers in 2017 alone.

Not long ago, for instance, Netgear fixed a bug that threatened to make administrative permissions available to hackers, according to Shah.

But there's a major catch. Consumers typically have to find, download, and install router updates themselves. And even computer experts rarely do that. A 2014 study (PDF) conducted by Tripwire found that fewer than half of IT professionals had recently updated the router firmware in their homes. Surprisingly, only 32 percent even knew how to do it.

That means that most home routers never get important security updates.
Instructions on how to update routers vary by brand, but for most models you need to log in to your router through a browser using the device's IP address. Here are links on how to update popular routers from Apple, Asus, D-Link, Linksys, and Netgear. Young's advice is to check for updates at least once per quarter.

You should also see if there's a way to get security notices via email from your router's manufacturer. The best way is to complete the product registration process, during which you'll be given the option to receive notifications when new software is available. Yes, that's definitely a chore, but it could save you a lot of trouble in the long run.

> Control those things you can, and keep the surprises to a minimum!