October 2020

Issue 8 Volume 10

frogworks

Managing your network so your business doesn't croak.

Run your business without worrying about technology

Ribb"IT" Review

INSIDE THIS ISSUE:

Before Twitter Patch, Private Messages May Have Been Vulnerable

If you're a Twitter user, you should know that the company recently announced that they had addressed a serious security flaw that could have allowed hackers to gain direct access to Direct or Private Messages users sent via Twitter.

If you seldom use that feature, then the impact to you would have been minimal in any case. If it's something you use on a regular basis, then breathe a sigh of relief.

The company had this to say about the issue:

"We recently discovered and fixed a vulnerability in Twitter for Android related to an underlying Android OS security issue affecting OS versions 8 and 9. Our understanding is 96 percent of people using Twitter for Android already have an Android security patch installed that protects them from this vulnerability.

For the other 4 percent, this vulnerability could allow an attacker, through a malicious app installed on your device, to access private Twitter data on your device (like Direct Messages) by working around Android system permissions that protect against this."

The company stressed that there's no evidence this security flaw was ever exploited in the wild, and again, there's nothing for you, as a Twitter user to do. The company has already handled it.

The discovery of the flaw though, comes on the heels of another recent, dramatic Twitter hack. In that hack, dozens of user accounts belonging to high-profile individuals were commandeered and used to bilk unsuspecting users out of more than $120,000 worth of Bitcoins.

If history is a good guide, and it usually is, this won't be the last major security flaw the company finds and addresses in what remains of the year. Nonetheless, kudos to Twitter for finding the flaw and acting quickly to correct it before it could be exploited. Here's hoping they can continue to find and correct them before the hackers can take advantage.

This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks

TECH TIP: Encryption

The best defense against theft is to have your device encrypted. Encryption won't prevent your device from being stolen, but it will protect the data residing on the device's hard drive from unauthorized access. Any data on an unencrypted device that is stolen would be considered accessible to the thief, resulting in a breach.

New Damaging Phishing Attacks Are Targeting Pandemic SBA Loans

The CISA (Cybersecurity & Infrastructure Security Agency) has recently published an advisory, warning of a new phishing campaign that specifically targets business owners who have received pandemic relief in the form of loans from the Small Business Administration. Apparently, according to the advisory, the campaign was launched toward the end of July 2020 by an as yet unknown group of hackers. It was altered slightly in the month of August.

In the initial wave of emails, the goal seemed to be to steal SBA login credentials. The latest effort focuses much more on attempting to trick recipients into providing a range of personal and financial information.

The campaign emails all bear subject lines that are some variant of "SBA Application - Review and Proceed" and comes from the (spoofed) email address: disastercustomerservice@sba.gov. A link embedded in the body of the email claims to take the recipient to the SBA signup where they will sign in to receive financial assistance. Naturally, the website is merely a spoof of the actual SBA page, replicated over a number of top level domains.

Security researchers tracking the campaign note that some of the phishing emails direct recipients to websites containing the GuLoader malware that is used to drop other malware payloads onto the machines of unsuspecting users. Researchers note that the most recent wave of emails use social engineering techniques that are sophisticated enough to fool even some security professionals.

If you are a business owner and have received pandemic relief or are considering applying for benefits, your best bet is to ignore any emails you might receive. Instead of clicking email links that promise to take you to the SBA's website, open a new browser tab and manually navigate your way there. It's a shame that hackers are taking such advantage at a time like this, but sadly, it's not much of a surprise.

Adobe Lightroom Update May Have Deleted Some User Photos

Recently, Adobe released version 5.4 of Lightroom. It is a popular photo editing app used by a wide range if iOS devices. Unfortunately, the update may have done more harm than good.

Many iOS users who installed the update have discovered that their photos and custom present filters were permanently deleted.

The only people spared from such a fate were those who paid for a subscription to sync their files to Adobe's cloud solution.

Rikk Flohr, an Adobe representative, confirmed that this was indeed a side effect of installing Lightroom version 5.4 on iOS devices. Curiously, the update for the Lightroom app on macOS and Android devices were not impacted in this manner.

If you have an iOS device and use Lightroom, don't install the 5.4 update. Adobe has subsequently released a fix in the form up Lightroom for iOS 5.4.1, which is confirmed not to delete user files.

Unfortunately, if you have already installed version 5.4 and you aren't paying for a subscription to the Adobe Cloud, the company confirms that there is no fix for the issue. Your lost photos simply cannot be recovered.

Needless to say, this is infuriating, and then some. Currently, there's a tremendous uproar on Reddit and other sites around the web, with some users having lost several years' worth of saved photos. Over the years, we've seen a number of botched updates that have led to a wide range of unexpected side effects ranging from the mildly annoying to the dangerous. Few have been as bad as this.

People cherish their photo collections and often have hundreds, or even thousands of digital memories. For a photo editing app to simply demolish all that in the blink of an eye is a weighty blow. It's going to take a long time for Adobe to win back the trust of the iOS community. It may not even be possible.

For now, just be sure to back up your photos or files in a few ways, just to be safe from unexpected incidents like these.

TECH TIP: Zoom Meetings

Before your meeting, reboot your internet and your computer to avoid any issues or interruptions during your call!

Security Issues Increasing With More People Working From Home

According to a recently published report by Malwarebytes, the global pandemic may be behind the recent surge in cyberattacks against businesses of all sizes.

While it wasn't immediately apparent, the pandemic forced businesses around the world to respond quickly to the emerging pandemic. As a result, tens of millions of workers began working from home.

In most cases, the infrastructure to make that possible was put in place very quickly, and as a result, the security surrounding that infrastructure wasn't as robust as it could have, or should have been. Hackers from around the world, always quick to take advantage of such situations, began striking at the new legions of homebound employees, finding easy pickings.

Based on the findings of the Malwarebytes research, nearly a quarter of organizations have found themselves having to pay unexpected costs to address malware infections or data breaches since shelter in place orders were imposed.

The three most common weak links were found to be:

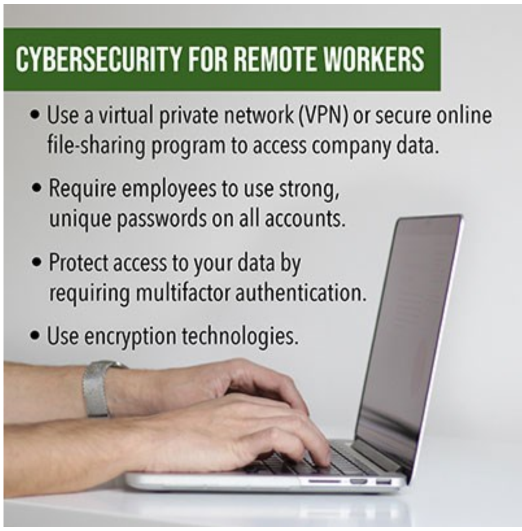
- Business eMail compromise
- Improperly configured security and access controls to cloud-based data
- Improperly secured corporate VPNs

That makes a certain amount of intuitive sense, given that in many cases, those are the kinds of things that would have been hastily rushed into place. It all went so fast, as businesses scrambled to respond to the new realities of the workplace which the pandemic imposed.

Adam Kujawa, one of the researchers responsible for the report, had this to say:

"Threat actors are adapting quickly as the landscape shifts to find new ways to capitalize on the remote workforce. We saw a substantial Increase in the use of cloud and collaboration tools, paired with concerns about the security of these tools. This tells us that we need to closely evaluate cybersecurity in relation to these tools, as well as the vulnerabilities of working in dispersed environments, in order to mitigate threats more effectively."

Wise words. If your business has seen a radical change in the way your employees work in recent months, and it probably has, now is the time to conduct a thorough security audit to limit your exposure.



CYBERSECURITY FOR REMOTE WORKERS

- Use a virtual private network (VPN) or secure online file-sharing program to access company data.
- Require employees to use strong, unique passwords on all accounts.
- Protect access to your data by requiring multifactor authentication.
- Use encryption technologies.

Amazon Moves A Step Closer To Delivery By Drone

For more than a decade, futurists have been talking about the day when drones will be used to deliver everything from packages to Pizzas. If you've been following the trends, you know that at least one major pizza chain has already begun experimenting with drone-based delivery. Now, Amazon's Prime Air drone delivery system has earned a critical FAA certification, which will allow it to begin testing customer drone deliveries in selected areas.

The simple truth is that Amazon is late to the party. Google's parent company Alphabet has a subsidiary called Wing that's already testing drone delivery, as is UPS. In other words, the future is here.

In Amazon's case, the certification in question is the FAA Part 135 cert, which allows operators to fly their drones out of direct line of sight.

David Carbon, the Vice President of Prime Air, had this to say about the certification:

"*This certification is an important step forward for Prime Air and indicates the FAA's confidence in Amazon's operating and safety procedures for an autonomous drone delivery service that will one day deliver packages to our customers around the world.*

We will continue to develop and refine our technology to fully integrate delivery drones into the airspace, and work closely with the FAA and other regulators around the world to realize our vision of 30 minute delivery."

If you haven't been following the story closely, you may not be aware, but Amazon actually drone-delivered their first package back in 2016, in Cambridge England. Since then, the company's drone pilots have logged thousands of hours of flight time, and the company has invested heavily in both drones and cargo aircraft in an effort to construct their own shipping and delivery network.

All that to say, it won't be long now before you get your first drone-delivered package from Amazon!

Tough times never last but tough people do.
– Robert H. Schiuller

We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter

and sign up.

ACCREDITED BUSINESS
BBB

We are excited and proud to announce that Frogworks has been accredited by the Better Business Bureau!

WE'VE MOVED!

2670 Crain Highway, Suite 304
Waldorf, MD 20601