frogworks
Managing Your Technology So Your Business Doesn't Croak.

# Ribb"IT" Review

"March is a month of expectation"

- Emily Dickinson

**March 2019**

Issue 3, Volume 9

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

***We are excited and proud to announce that Frogworks has been recognized as one of the world's best MSPs by Channel Futures!***

Channel Futures MSP 501 2018 WINNER

THE ULTIMATE GUIDE TO THE WORLD'S BEST MSPs

## Large Increase In Business Email Hacking Incidents

Given the rate of increase in the number of hacking attacks, it was predicted early on that 2018 would be another record setting year. That came with more hack attempts and more successful attacks than were seen in 2017. Sadly, that prediction proved to be correct.

What few people had anticipated, however, was how big of an increase we'd see.

While the number of attacks generally increased throughout 2018, few areas saw more explosive growth than BEC, which stands for Business Email Compromise attacks. Those hacks accounted for a mind-boggling 476 percent surge between the fourth quarter of 2017 and the fourth quarter of 2018. To give that number some context, by comparison, the number of email fraud attempts against businesses also increased by by just 226 percent over the same period, which while staggering, is paltry by comparison.

BEC attacks therefore win the dubious honor of being the fastest growing security risk on the current threat matrix, and the most likely type of attack that businesses are likely to experience.

These are, at their core, social engineering attacks that target specific employees of a firm, typically in the company's finance department. The goal is to convince them that they're dealing with a vendor the company regularly does business with and convince them to send large sums of money. This is typically via wire transfer to accounts that, at first glance, appear to be legitimate vendor accounts, but which of course are controlled by the attackers.

While less sophisticated attacks rely on poisoned files or URLs to do their damage, these attacks rely on trust and psychology. As such, they're significantly more difficult to spot, which is one of the many reasons they can be so devastating. By the time the victims realize what has happened, it's far too late.

Vigilance is the only real way to combat this form of attack, so be sure your employees understand the risks and that they are are on their guard. Lastly, verify any significant transfer of funds in person. Better to be safe than sorry.

# New 5GE Coming To Phones Is Still In Development


AT&T is getting some pushback for what most industry insiders are calling a misleading indicator. It has started to appear on many new smartphones including both Androids and iPhones. With the latest update, a growing number of customers are now seeing a "5G E" indicator on their 4G phones, which leads to a momentary surge of excitement, leading customers to believe they're using 5G technology.

The indicator actually stands for 5G Evolution. It's still 4G technology. It does have some enhanced features not found on other 4G devices, including 256 QAN, 4x4 MIMO and three-way carrier aggregation. Even so, it's a far cry from being 5G technology, which isn't slated to roll out until sometime in 2020.

**AT&T defended the move with the following statement:**

"5G Evolution is our first step on the road to 5G. It is now live in over 400 markets with more to come, and soon our most popular smartphones will start displaying the 5G E indicator to let you know when 5G Evolution coverage is available."

Both users and the company's competitors have widely mocked the indicator. Customers expressed a range of emotion that spans from frustration to outrage. For the time being at least, AT&T is sticking to its guns and shows no signs of backing away from the indicator. In fact, AT&T Communications CEO John Donovan dismissed the complaints by saying simply "Our competitors are frustrated."

They're not the only ones. Although at this point, it's unclear what (if any) backlash the company will face courtesy of unhappy customers.

Honestly, although the move is ham-fisted and a bit deceptive, AT&T isn't likely to lose many, if any customers over the issue. It is something of a public relations black eye. Long story short though, don't be fooled by the new indicator. 5G is still quite some distance away.

# Google+ is Finally Getting Deleted

Google has kept no secret of their plan to eventually put an end to their social media experiment, Google+. In case you haven't been keeping abreast of the company's announcements where the service is concerned, be aware that it will be shutting down on April 2nd of 2019.

The closer we've gotten to that deadline, the more details we've gotten from the company about how the shutdown will go.

Just so you're aware, this won't be a simple matter of turning off access and freezing posts as they are, or essentially preserving them for all time. No, this is going to be an internet-wide absolute deletion of any and everything related to Google Plus.

That means your posts, your comments to other people's posts and your Google+ powered comments on Blogger

*(Continued on page 3)*

*(Continued from page 2)*

and other blogging sites will all ultimately be deleted. If you want to preserve any of your materials, it's long past time to start archiving. You've still got time of course, but the clock is ticking more loudly than ever now, and depending on how much content you've got, you'll want to be quick about it.

Google+ never enjoyed the kind of popular success that Facebook and the other heavy hitters in the social media ecosystem enjoyed. It was more of a panicked reaction to the meteoric rise of Facebook, with the fear being that Facebook might kill search if everybody simply gravitated to asking their friends for recommendations.

Obviously nothing like that happened, but it was of genuine concern when the company launched the service, and it's what prompted them to inject Google+ into every aspect of their product ecosystem, even in cases where it didn't make much sense to do so.

Given this deep integration, shutting down Google+ and deleting all traces of it won't be a quick or easy process, but it's coming, and that starts on April 2nd. Note: The shutdown applies to consumers only. Enterprise users will still have access to Google+ functionality via the G Suite.

## GSuite Now Offers Better Android Mobile App Management Options

GSuite has added an important new bit of functionality in the form of Android App Management, which comes in two basic flavors. There are some things you can do using the company's basic app management console, but to get access to the full range of features, you'll need to set up an advanced account. It's a significant and most welcome change indeed, enabling a whole host of new features. Here's the quick breakdown.

**Using the basic app management feature, admins can now:**


- Maintain a device inventory
- Enable basic password enforcement
- Gain access to mobile reports
- Enable hijacking protection
- Perform remote account wipes on company devices
- Create a list of apps that can be installed on work devices

**The advanced management console allows all of the above plus:**

- Standard and strong password enforcement
- Device approvals
- Strategic blocking of devices
- Remote device wipes

*(Continued on page 4)*

### Google Is Rolling Out New Features For Gmail Users

Google has recently announced a trio of new features for Gmail users that are going into place immediately, and may in fact be available for use by the time you read this article. Here are the details:

One of the first things you'll notice is a new strikethrough button, visible when you're composing. You'll find it on the right-hand side of the menu.

Per Google's statement about the new additions, "Strikethrough is a visual cue that something has been completed or can be used as an edit suggestion. We've heard from you that this functionality is critical to quickly and efficiently write emails, especially when you want to visually indicate a change in language."

In a similar vein where edits are concerned, the company is also introducing an "Undo/Redo" button, which will allow Gmail's email compose screen to function more like a conventional word processor. Undo/Redo is incredibly handy in those instances where you intended to copy a block of text and deleted it by mistake instead.

Finally, the company is now allowing its users to download their emails as EML files for remote or offline viewing. EML files are compatible with most major email clients, leaving open the possibility of sending them in batches to yourself or someone else who is authorized to received them. The download can be accomplished by clicking on the three dot menu and selecting "Download Message" at the bottom of the menu.

Again, by the time you read this article, the changes may already be in place for all Gmail and GSuite users, so be sure to check them out to see if you find them helpful.

The early buzz is quite positive for all three changes, with the Strikethrough functionality having been on several people's wish lists for quite some time. Kudos to Google for listening to their user base and making the changes.

- iOS App management
- Android work profiles which allow you to create different allowed apps on a per profile basis
- Device audits and alerts
- Establish device management rules and security policies
- Bulk enrollments for company-owned desktops and Android devices

In addition to that, Admins will now be able to remotely install apps on any user device and prevent users from uninstalling apps. You even have the option to create your own web or private apps as needed. This is huge because a private app does not need to be run through the same checks and security protocols as an app that's destined for an appearance on the Play Store account, which means you won't even have to create a Play Store Console account if you don't already have one. GSuite just keeps getting better and better. Kudos to Google for the latest changes. Managing your company's digital assets has never been easier.

## Google Releasing Chrome Extension To Detect Password Theft

Google has a new extension for its Chrome browser, and it's one you should strongly consider getting for all of your devices at home and in the office.


The extension is called 'Password Checkup,' and has exactly one purpose. It securely checks your logins against a breach database in real time as you're logging onto the various websites you use daily.

Note that the plugin checks both passwords you enter manually and those stored in Chrome's password manager.

It's a brilliant feature, although not without risks. After all, it opens up the possibility that during the check procedure, your password could be detected by a hacker monitoring your device. Even so, the risks of that happening are quite small, while the benefits gained via getting real time information about whether your passwords have been compromised is too big to ignore.

The central issue is this: Over the past several years there have been scores of high-profile data breaches that have seen literally billions of user ID's and credentials exposed, most of which wind up for sale on the Dark Web. Worse, most users are blissfully unaware of the fact that their credentials have been compromised. This extension changes that, giving you an opportunity right then and there to change your password.

The development team is constantly updating the massive database that the extension uses to check for compromised passwords, and they've got plans to extend the use of the API's capabilities down the road. They're even shopping for suggestions from Google's vast user base on how best to use it in future projects.

Overall, despite the fact that the new extension opens up potential for abuse, the availability of the new capability is hailed as a great step toward better security.