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

Ribb"IT" Review

> "Information is the oxygen of the modern age. It seeps through the walls topped by barbed wire, it wafts across the electrified borders."
>
> -Ronald Reagan

June 2020

Issue 4, Volume 10

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

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

BBB ACCREDITED BUSINESS

Google Added A Video Conferencing Tool For Users

Google Meet is a video conferencing tool the company originally designed for Enterprise users.

There are serious security issues with some of the more popular free or low-cost options available for the masses.

So, Google made the decision to make Meet free to anyone with an email address.

The rollout took two weeks to complete, but is now available to all. It can be yours simply by heading to meet.google.com, or by paying a visit to the Google Play or Apple App store.

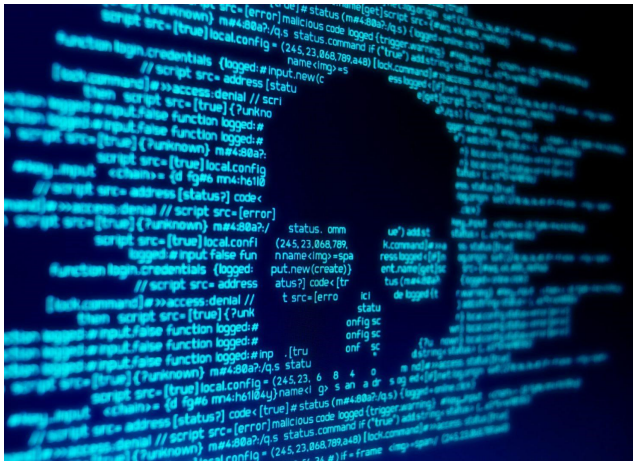
Since the global pandemic forced so many people to work from home, Google has seen a huge surge in demand for the service. Last month alone, Meet added an average of 3 million new users a day. Seeking to further capitalize on the increased demand, the company is taking steps to make their offering even more attractive. They are among other things, adding a new feature that makes it directly accessible from Gmail.

Google isn't alone in the rush to capture an increasing percentage of this burgeoning new market. Last month, Facebook announced a whole raft of new video products, including Messenger Rooms. Rooms are consumer-focused video conferencing solutions that leverage the company's well-established technology.

Even with the rush of competition into this sphere however, Google is well-positioned to utterly dominate the market. The G-Suite is incredibly popular among Enterprise users. By opening Meet's features up to the general public, the company should be able to capture a significant portion of the new demand for home video conferencing services.

Even after the pandemic is behind us, industry experts are predicting that there won't be much of a decline in demand, and that video conferencing will come to increasingly define the way the world works. Only time will tell. Meanwhile, if you're a fan of the Google ecosystem, you can get your hands on a new, high value video conferencing tool for free.

Well-Known Tech Support Scam Traced to India



I think we've all seen those virus alerts to some degree or another that pop-up on our desktops telling us that we've been infected. They'll typically pretend to be from legitimate companies like Symantec or Microsoft (in some cases, even using a fake Microsoft logo to establish credibility), and they always want you to call a fake number — which leads to paying money for a fake service.

I'd like to believe that anyone reading this blog is someone who can detect this kind of scam, but regardless, whether you've fallen for this in the past or not, new information on the source of this costly annoyance appears to have come to light.

And it takes us all the way to India, thanks to The New York Times.

The article begins by telling us that 1 out of 5 people who receive such alerts tend to contact the fake tech support centers, while 6% of users in general actually pay for the fake services – which is crazy in and of itself.

Nothing about those alerts look legitimate, but hey, there are A LOT of people on this planet…

The meat of the piece points to Microsoft and how they helped police trace who was behind these large-scale operations. Apparently, these scammers have their roots in New Delhi, the capital of India, which is also the epicenter of call centers in general.

According to the software giant, more than 11,000 calls per month about fake security warnings were being received. And many people as a result, lost significant sums of money to the fraud.

On Tuesday and Wednesday, police from two New Delhi suburbs raided 16 fake call centers and arrested more than 50 in connection with the scam.

The Scam

Fixing the non-existent virus could involve calling a tech support center, where an operator would talk a victim through a fake fix and then charge them for the work. In other cases, the bogus tech support team would call their targets themselves and pretend to be a Microsoft employee, bringing to their attention a virus or false claim that his or her system could have been hacked. Eventually, they ask for anywhere from $99 to $1,000 to fix the problem that doesn't exist in reality.

Courtney Gregoire, an assistant general counsel in Microsoft's digital crimes unit, perhaps said it best when she was quoted as saying, "This is an organized crime." No doubt.

The scam is incredibly lucrative according to researchers at Stony Brook University. They published a detailed study of fake tech support services last year that estimated just a single pop-up campaign, spread over 142 web domains, could bring in nearly $10 million in just 2 months.

Microsoft said it was working with other tech industry leaders such as Apple and Google, as well as law enforcement, to fight the digital epidemic, which is migrating beyond the English-speaking world to target other users in their local languages.

Microsoft has also published advice about ways to spot the fake calls and avoid becoming a victim.

We now have an E-newsletter!

… but we might not have your email address!

Twitter discloses privacy issue that caused caching of files sent via Direct Messages in Firefox

Twitter admitted that the private files sent via Twitter DMs were cached inside the users' Firefox browsers for up to seven days, even if users have logged off.

The problem is related to the way the Mozilla Firefox web browser cached data. This caused the storage of private media shared in DMs and data downloads in the browser's cache.

An attacker could have accessed private data stored in the Firefox cache using specific tools.

"We recently learned that the way Mozilla Firefox stores cached data may have resulted in non-public information being inadvertently stored in the browser's cache," reads the announcement published by the company.

"This means that if you accessed Twitter from a shared or public computer via Mozilla Firefox and took actions like downloading your Twitter data archive or sending or receiving media via Direct Message, this information may have been stored in the browser's cache even after you logged out of Twitter."

The privacy issue doesn't affect other browsers such as Google Chrome and Safari.

Mozilla implemented a retention period of 7 days in the Firefox browser, this means that the content of the cache is automatically being deleted after a week.

Twitter announced that it has addressed the issue, Firefox will no longer store users' personal information in the browser cache.

"We have implemented a change on our end so that going forward the Firefox browser cache will no longer store your personal information." continues Twitter.

"If you use, or have used, a public or shared computer to access Twitter, we encourage you to clear the browser cache before logging out, and to be cautious about the personal information you download on a computer that other people use."

Options > Privacy & Security > Cookies and Site Data > Clear Data. Uncheck the *Cookies and Site Data* option and only check *Cached Web Content* and then click the *Clear* button.

Videos In Google Photos Accounts May Have Been Exposed

Security lapses can happen to any company, large or small. No one is immune. Not even Google. Recently, the company began sending out email notifications to some users explaining that a bug in their system caused their videos to be shared with other users.

Their email notification reads in part as follows:

"...some videos in Google Photos were incorrectly exported to unrelated users' archives. One or more videos in your Google Photos account was affected by this issue."

In particular, the issue is centered around the Google Takeout service, and occurred between November 21st, 2019 and November 25th, 2019. Any user who used Takeout during that period may have received videos that do not belong to them.

The company spotted and fixed the issue, so there's nothing to worry about going forward. However, if you used Google Takeout during the dates mentioned above, you'll want to do another import now to be sure you got everything.

This is a big deal for a few different reasons. Naturally, people who store their photos and videos on Google Photos expect them to remain private. Clearly in this case, that didn't happen. If you use the service to store videos that you don't want anyone to see, that could be a problem.

It also underscores the inherent risks involved in storing your data on the cloud. Yes, it's convenient. Yes, it saves space on your phone. Those are good things, but there's a trade off, and sometimes, that trade off is a painful one.

There are no perfect solutions here. Although such lapses in security are rare at Google, they do happen. They'll continue to happen. Each person using cloud-based storage solutions will have to come to find his or her own balance between privacy, security and convenience, which is no easy task.

Some Smart Light Bulbs Are Vulnerable To Hackers

Hackers will take any and every opportunity presented to them, even if it means hacking smart light bulbs. Recently, security researchers at Check Point discovered a bug in the Philips Hue smart bulb that makes it vulnerable.

The bug is being tracked as CVE-2020-6007 and scores an impressive 7.9 out of 10, making it the most serious security flaw in a light bulb we've ever seen.

It sounds funny. After all, who would want to hack a light bulb? But it's actually got serious implications. After all, the light bulb is just the beginning. Once hackers are 'in' the bulb, it gives them a beach head on the network that the bulb is attached to, and from there, they can jump to any other device they can see.

Fortunately, Philips has already published a fix for this, in the form of firmware version 1935144040. If you own one or more Philips Hue bulbs, you'll want to check the firmware version. If yours has not already been updated, take the time to do so.

This underscores the one glaring weakness of the Internet of Things. Very few of the smart products we're connecting to our networks have any security at all. The few devices that do boast some kind of security often have flaws like the one discovered here, which are severe enough to be considered crippling.

The net effect is to make any network that incorporates smart devices much less secure. After all, your network is only as secure as the weakest device on it, and smart devices have notoriously bad security.

That's changing, but it's changing at an incredibly slow rate. If you've got smart devices on your network, consider isolating them and minimizing the amount of contact they have with other devices on your network. That way, at least you can mitigate the impact until security improves.

Wishbone App Database Leaked To Public By Hacker

The hacking group calling themselves 'The Shiny Hunters' has been busy.

Recently, they put databases containing user records from eleven different companies up for sale on the Dark Web, including a massive database containing some 40 million records belonging to the popular Wishbone app.

Wishbone is a social media platform that's especially popular among children. It allows users to compare two items by way of a simple poll. The database was initially being offered for 0.85 bitcoin, which is, at the time this article was written, worth approximately $8,000.

Only days after the database was originally offered for sale, it appeared elsewhere on the Dark Web in its entirety, for free. The information it contains includes usernames, email addresses, phone numbers, geo-location data, hashed passwords, and profile data, including links to uploaded user photos. That's bad news indeed for any parent, because again, this app is especially popular among children.

A closer inspection of the records the database contains reveals that the hashed passwords are only weakly encrypted, using MD5, which can easily be broken using freely available tools, putting every one of the 40 million users identified in the database at risk. If you're not sure if your child has downloaded Wishbone, it pays to double check immediately. Be sure to change the password on any account you or your children may have associated with the account. For the company's part, a notice recently went up on the Wishbone website that read: *"Protecting data is of the utmost importance. We are Investigating this matter and will share any significant developments."* Unfortunately, the most significant development is that some 40 million of the app's users are now at risk. Don't take any chances. If you or your kids use this app, change your password immediately and be on the alert for phishing emails sent to any email address referenced in your Wishbone profile.