November 2020

Issue 9 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:

Microsoft Considering Adding Meet Now Button For Online Meetings

The Coronavirus pandemic has changed a number of things about how the world works.

One of the bigger and more noticeable changes is, of course, the fact that so many people are working from home these days. They're relying on video conferencing software in lieu of face to face meetings.

This year, Google and Microsoft have seen tremendous growth in the use of their videoconferencing services. However, it is plucky upstart companies like Zoom that have been the real trailblazers, leaving the tech giants to play catch-up.

The tech giants might have been a bit slow to respond to the changing paradigm, but they've got the resources to do it right. Recently, Microsoft has made changes to Skype that indicate the company is ready, willing and able compete head to head with Zoom.

Among the recent changes the company has rolled out is the new "MeetNow" feature in Skype, which is a new icon that resides in the system tray of Windows 10, allowing for one touch convenience when setting up a new video call. No need to log in, just click the button and you're off and running.

The new feature is generating a lot of buzz for Microsoft, and if you'd like to see it in action and test it out for yourself, and if you're a Windows Insider, just grab a copy of Windows 10 Build 20221 and install it. Be sure to check out the company's blog post about the build, which contains a complete list of newly enhanced functionality as well as a list of known issues with the new services.

In a related vein, Microsoft has also recently added a new feature to its "Your Phone" app, which allows users to pin important notifications to the top of the notifications feed. A small change, but a very good one.

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

In any case, Windows Insiders can get a sneak peek at the new functionality right now. The rest of us will have to wait until some future build to see what the company has been up to on the videoconferencing front.

Running And Bicycling App May Be Sharing Personal Data

Do you use the Strava app when you run or bike?

If so, it may be sharing your personal information in ways you hadn't expected.

Andrew Seward, the head of Data and Product Development at Experian was out for a morning run when he noticed something so unusual that he felt compelled to tweet about it.

While on his morning run, he passed a woman who was also out for a run and who happened to be using the Strava app herself. When he got home, he found that the woman's face appeared in his app as someone he ran with, even though they didn't know each other and weren't following each other in the app.

Clicking on her face brought up her profile and the route she ran, which essentially pointed the way right to her front door. That's disturbing to say the least, and Seward's tweet sparked a firestorm of controversy about the app.

As it happens, it's a feature, not a bug. The app has a feature called "Flyby," which is designed to do exactly what the app did in this instance. Unfortunately, Flyby is set to "everyone can see you" by default for all users.

Fortunately, the app does offer controls that allow users to filter who can see them, but it's not apparent that the feature is set to "everyone". Unless you happen to check, you may not even be aware that your information is being broadcast to every other Strava user you run or bike past.

If you're feeling a touch of paranoia reading this article, there's an easy way to check the app to see who can see you. Here's how:

- Just log in and go to settings.
- From there, tap "Privacy Controls."
- Scroll down until you see the "Flyby" section and set it to your liking or, to turn it off, select "No One."
- Tap Ok to save your changes.

That's all there is to it, and it will give you tremendous peace of mind!

Facebook Working On Business Suite For Managing Social Media

Social Media giant Facebook, recently announced a new app aimed at Enterprise users.

If you maintain an active corporate presence on Facebook and Instagram, you'll be particularly interested in the company's new offering.

It is designed to give business owners a dashboard that will make it easier to manage their company's social media presence, allowing users to post simultaneously to both Facebook and Instagram and receive notifications and alerts related to both platforms in a single location.

Sheryl Sandberg, the COO of Facebook, had this to say about the new app:

"We're building Facebook Business Suite for small businesses first, but this is a long-term investment to make this the main interface for businesses of all sizes who use Facebook, Messenger, Instagram and WhatsApp. It is available for small businesses globally starting today and will expand to larger businesses next year."

The new Business Suite is the latest in a series of moves the company has been making in recent months as it pushes more earnestly into e-commerce. In May of this year (2020), the company rolled out a new set of tools allowing business owners to set up a digital storefront on Facebook and sell goods and services to their followers.

As Facebook's CEO Mark Zuckerberg recently noted, companies of all sizes have made significant investments into their digital footprints and are *"increasingly viewing them as their primary storefronts. So we're working on a number of ways to deepen this experience, helping people buy items and services directly within our apps... Overall, though, our business depends on the success of small businesses, so this is a moment where we feel that we're well-positioned to be champions for small business' interests and supporters of important infrastructure that they're going to need in order to move online."*

The bottom line is, if you use Facebook and/or Instagram, the new Business Suite is well worth a look.

New Updates For Office 365 Will Include Phishing Protection

Are you an Office 365 user? If so, be aware that Microsoft is adding some powerful new protections to the software suite, designed to make you safer.

Hackers commonly target Office 365 users with a type of attack known as "Consent Phishing." That basically means that the hacker in question will use a variety of social engineering techniques to try and trick a target victim into giving up his or her Office 365 access, usually by way of an app that asks for permissions. If the user grants those permissions, the app can install all manner of malware on the target's device.

The new security upgrades that Microsoft is rolling out makes users safer in three different ways:

- First by a general tightening of app consent policies
- Second, by placing a greater level of scrutiny on publishers of OAuth apps during the verification process
- Third, by changing the rules surrounding user consent when consent is asked for by an unverified publisher

These changes are already in place, and since their initial rollout, Microsoft has verified more than 700 different app publishers and more than 1300 individual apps. Verified apps can be recognized by the small blue badge with a white check mark in its center. Those apps, you can install with confidence.

As a Microsoft representative explained:

"To reduce the risk of malicious applications attempting to trick users into granting them access to your organization's data, we recommend that you allow user consent only for applications that have been published by a verified publisher."

It's good advice, and these are excellent (even if they're somewhat overdue) changes to the company's policies. Kudos to Microsoft for rolling out the upgrades to their processes, and to the legitimate publishers who are already moving to embrace the recent changes. This will help keep users safe, and that's a very good thing.

Every strike brings me closer to the next home run.

–Babe Ruth

TECH TIP: SPOOFING

Email spoofing is common in phishing emails. Scammers will take a well-known email address and adjust a letter or two, hoping you miss it. Example: billing@nationalbrank.com.

Caller-ID spoofing is when scammers manipulate the phone number they are calling from. By using a verified legitimate business phone number or a similar number to your own, the likelihood of you picking up the call increases dramatically.

Website spoofing is a scammer's way of getting you to think you are at a trusted website. By mimicking the look and feel of a real website, you are more likely to provide

Staples May Have Exposed Some Of Its Customer Data

If you're a customer of US retail chain Staples, you may have recently received a notification from the company regarding a problem with their Order Tracking system.

According to information in the notification, the data was left exposed due to insufficient protections of the data stream accessed when a customer clicked to review their current and past orders.

The company stressed that to this point, there is no evidence that any exposed data has been accessed by third parties and no unauthorized purchases have been detected.

Although the company has now fixed the issue, the lack of specifics in the company notification led to speculation that the company may have been hacked. This speculation was given teeth by a recent tweet from the threat intelligence company, Bad Packets. They revealed that Staples was slow to patch a number of their Pulse Secure VPN servers, which were vulnerable to CVE-2019-11510.

Although the company has neither confirmed or denied the claim made by Bad Packets, the company outlined an all too plausible way that a hacker could have accessed order data, including the order's shipping address.

Here's how that could have happened:

Staples' order tracking portal allows you to enter in your zip code and order number to track your package, but the order numbers are sequential. So starting with an exposed order number, a hacker could access the route of a package to the city and state, which would give them a short list of possible zip codes. Trial and error would do the rest, and the hacker would end up with your name, address, and at least some information about how you paid for the purchase, although payment card information itself would not have been exposed.

In any case, it's all speculation and the issue has been fixed. Out of an abundance of caution, if you are a Staples customer, keep a watchful eye out on the payment card you use to make purchases from the company, and track your existing orders more closely to be sure you get everything you paid for.

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.

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