COMPUTER NEWS from the

Titusville Computer Community

Titusville, FL

FEBURARY 2018 Volume 6 NO. 2

As found on the web and other sources

Most Dangerous Security Threats of 2018?

Category: Security From “askbobrankin.com”.

What will be the biggest security threats of 2018? Would it surprise you to learn that YOU might be on the list? Read on to learn about the threats to your privacy and security that are most likely to impact you in the coming year…

Are You Part of the Problem or the Solution?

Ransomware and “people” topped a survey of security pros’ predictions of the biggest cyber-security threats the world will face in 2018. But among the 72 respondents to research firm IDG’s question, there are more specific responses and a few threats that are less than obvious. The latter, I think, may be the more dangerous threats. Read on to learn more.

Ransomware is a proven money-maker for scammers. By encrypting the precious data of a corporation, organization or end user, ransomware inflicts immediate and severe pain. The promise of getting data back quickly by paying a ransom is keenly compelling. Additionally, ransomware and its attendant "victim relationship management" apps are now bundled into easy-to-use "Software-as-a-Service" sites that any aspiring blackmailer with a couple of hundred dollars can rent. So there will be exponentially more ransomware attacks launched in 2018.

The targets of ransomware are predicted to shift from low-value individuals and small businesses to major corporate and government systems. A crook can charge much more for the encryption key to bigger and more critical systems. Targeting key executives within a large organization with carefully crafted phishing emails is becoming a fine art among criminals.

That leads us into the "people" security risk, which IDG's respondents cited 12 times to ransomware's 11. There are many ways that human error can allow bad actors into a system whose hardware and software are well protected. You, faithful reader, may already know all about them. But the growing threat to you and your precious data is the staff of the online entities with which you do business.

Front-line employees are under ever-increasing pressure to produce more, leaving them virtually no time to think about whether they should click on the attachment to an angry "customer" complaint, or the link to a web page purportedly showing the cause for the complaint. Many of these staffers are unhappy, underpaid, and ripe to either cause their employers trouble or be recruited by bad actors in exchange for money.

Management, up to the C-level, doesn't do enough to train staff in best security practices, enforce them, and demand that software systems prevent staffers from doing things that can let crooks in the door. Even IT staffers, who know better, fail to apply patches to software promptly.

An Ounce of Prevention...

In the recent Equifax data breach scandal, it was discovered that a directive to apply a simple patch that would have protected the credit histories of over 140 million Americans went ignored for at least two months. I surmise that the derelict IT employee was not irresponsibly negligent, but simply could not find time to apply the patch without "disrupting" normal business operations, which would have gotten him in trouble.

The insenstivity to security extends across supply chains. As firms become more closely integrated with their partners, a security vulnerability in one member of the group becomes a hazard to all members. Yet very little is being done by any given firm to vet the cyber-security of suppliers and large customers.

The oldest networked information systems, including critical utilities, financial services, and health care providers, are generally the most vulnerable to modern hacking threats. The industrial controls that govern the flows of water, electricity, and even street traffic were designed with only the crudest password protection, if any.

The Internet of Things is the fastest-growing “attack surface” for hackers on Earth. The makers of light bulbs, refrigerators, and coffee pots know nothing about cyber-security and don’t want to pay for pros who do. Even Amazon Key, the company’s latest “smart” innovation, allows delivery people to open the door to your home. But it launched with an easily-exploited flaw that would let a nefarious delivery driver walk off with the entire contents of a customer’s house.

“The IoT-connected world that surrounds each and every one of us is getting more complex, sharing more of our data in evermore opaque ways and getting less easy for the average user to understand, let alone to have any hope of controlling a perfect security storm,” wrote Nigel Harrison, CEO at Cyber Security Challenge UK, in his response to IDG’s survey.

Simply banning “smart” gadgets from your home is not a perfect defense, although it will reduce the attack surface your home network presents to bad actors. You have no choice about the software that the electric company uses in its smart meters, or the security practices of the public works department that controls water delivery and traffic signals, or the practices of 911 system administrators. You don’t even know what your car’s computer is doing under the hood, or how it can be hacked to kill you.

What you can do, and I urge you to do, is apply unrelenting pressure upon your government representatives and business partners - banks, Amazon, et. al. - to publicly demonstrate how they are acting to protect their systems upon which your livelihood and life increasingly depend.

Back to the YOU Part of the Security Picture

It never hurts to repeat a few personal security mantras. Below are some links to other AskBob articles that will help you tighten up your own defenses, and ensure that "YOU" are not on the list of the most dangerous security problems in 2018.

- Keep Your Software Updated
- Use Anti-Malware Protection
- Create Strong Passwords
- Use Two-Factor Authentication
- Guard Against Phishing Attacks
- Backup your data!

Your thoughts on this topic are welcome.
Post your comment or questions to “askbobrankin.com”.

Firefox Quantum: Comeback or Flameout?

Category: Browsers in “askbobrankin.com”.

Firefox is poised to make a comeback, at least among fans who switched to Chrome only reluctantly. The public beta version of Firefox 57, also known as Firefox Quantum, is now available to download and test drive. It really is pretty impressive. Let's take a closer look...

What is Firefox Quantum?

Several years ago, Firefox lost a lot of ground in the battle for browser market share when its developer, The Mozilla Foundation, let the browser grow fat and slow while chasing multiple dreams that never became reality (a mobile phone operating system, IoT services, creating a built-in video chat service, etc.). But the development team has returned to its roots, and the result is truly a quantum leap above previous Firefox versions.

Firefox Quantum renders pages up to two times faster than the previous version, according to the company. A large chunk of this performance improvement is credited to Firefox’s new ability to take advantage of multi-core processors and a new CSS engine.

My own subjective impression is that Quantum is roughly equal to Chrome in rendering speed now, and switching between tabs is much zippier, too. Firefox Quantum uses much less RAM than previous versions and certainly less than Chrome.

The headline of a Mozilla blog post declares: "Firefox Quantum is super fast, while still conserving memory." You can see charts comparing the performance of Quantum to the previous version of Firefox. But curiously, they do not include any head-to-head comparisons of Quantum to Chrome, Edge, Internet Explorer, Opera, or Safari.

Mozilla says "results will vary based on your computer and the apps you're using," but my guess is that older and low-end machines will see the most performance gains with Firefox Quantum. Test results showed that Quantum used about 30% less RAM memory than Chrome on Windows, but slightly more than Chrome on a MacOS system.

You can view the test results in the blog post linked above, and try the Speedometer benchmark test yourself, to see how the new Firefox performs, compared to the browser you have now.

A Few Cosmetic Changes, Too

The user interface has also changed. Gone are the rounded corners on tabs and buttons, providing a much cleaner and modern look. It also renders better on high-dpi screens found on modern laptops and touchscreens. Firefox Quantum can still be customized to one's heart's content, from scratch or using skin templates available on the Mozilla site.

Firefox Quantum still includes Pocket, which stores pages for offline reading, and the Reading Mode that strips extraneous content out of a page for easier concentration on the text. A handy instant-screenshot function is a nice addition. And of course, you can still use third-party extensions to add features and customize your 'Fox.

Will it Reverse the Death Spiral?

Is Firefox Quantum good enough to wrestle market share away from Chrome or Internet Explorer? I think it will entice only that small group of users who wistfully miss Firefox but switched to Chrome when Firefox became fat and slow. People who use many Google services such as GMail, Docs, Photos, Drive, etc., will stick with Chrome because it provides better integration with the services they love. It's not so much the browser's performance that dictates their choice, but what they can do with Chrome.

However, Firefox Quantum may be able to slow the precipitous decline of Firefox's market share, which currently stands at just under 13% (versus 22% a year ago). Market researchers at StatCounter have projected that Chrome will virtually obliterate Firefox and Internet Explorer by 2019; Quantum may push that death date out a bit. Quantum should also give Firefox a leg up over Safari, Opera, Edge, and other bit players.

Firefox Quantum is still in Beta test mode, and will be released on November 14, 2017. You can download it now and take it for a spin, or sign up for updates by email. Look for the blue "Keep me updated" button at the bottom of the Firefox Quantum page.

Your thoughts on this topic are welcome. Post your comment or question to askbobrankin.com..

HELP, I've fallen and can't get up!

Man dies in VR accident, reports Russian news agency

By Tyler Wilde in "askbobrankin.com".

This is the first VR-related death we're aware of.

- –

Getty Images

A 44-year-old Moscow resident died after falling through a glass table while wearing a virtual reality headset, reports Russian news agency TASS.

"According to preliminary information, while moving around the apartment in virtual reality glasses, the man tripped and crashed into a glass table, suffered wounds and died on the spot from a loss of blood," said Yulia Ivanova, Senior Assistant to the Head of the Russian Investigative Committee’s Main Moscow Department, according to TASS. The report does not include details about the type of VR headset the man was using, or what he was using it for.

This is the first report of a VR-related death we've heard. The article came to our attention after it was spotted by Reddit user daio earlier today. TASS is a state-owned news agency, and the largest in Russia.

Found but not tried, use at your own risk!

Get This Ad Blocker That Works Across Apps and Browsers on Android

toggle-button From gizmo’s freeware

Submitted by Jojo Yee | Last update on 3rd December, 2017 - 4:24am

When you see ads on a website or in an app, it generates some revenue to the publishers who use it to cover part of the cost of providing content and do not need to restrict it to a paid subscription.

Sensibly most people don't like ads and treat them as an unwanted distraction. To do away with ads, you may install an ad blocker in a browser but, in turn, some publishers start to hide content from viewing unless you whitelist their websites from ad-blocking.

Regardless who wins the race, it's probably a noble act to support a reputable website or an app that you love and regularly go to without blocking its ads.

If you are looking for an ad blocker that has a whitelisting feature and works on non-rooted Android devices, then check out this DNS-based ad blocker **Blokada**. It effectively blocks most ads and tracking across browsers and apps.

Just like TubeMate YouTube Downloader, Blokada is not available from the Play Store as they are regarded as interfering with Google's business model. Get Blokada from the developer's site instead and allow installation of this app from sources other than the Play Store.

This app is free, open source and scanned clean on VirusTotal. Many thanks to Panzer for recommending this app.

Facebook Wants Your Face and You'll Probably Let Them Have It

By Sidney Fussell in "gizmodo.com".

Photo: AP

Facebook just got one step closer to becoming the literal embodiment of its name. On Tuesday, the company announced it's rolling out several new facial recognition features on its platforms. Once you agree to let Facebook use your face data, you gain access to new tools the company says will help protect your privacy and block catfishing attempts.

In a blog post, the company described the new features that will soon be available to users who turn face recognition on with "a simple on/off switch":

1. Facebook will alert you when photos of you are uploaded, even if you haven't been tagged in them. This happens even if you aren't friends with the person who uploaded the photo, so long as you're included the audience group specified by the uploader's privacy settings.

2. Facebook will alert you if your face is included in a profile picture. This update is aimed squarely at preventing catfishing and “revenge porn” style attacks, where someone creates a fake profile using intimate photos of a person without their consent.
3. Finally, visually impaired users can now hear aloud who’s tagged in photos alongside them.

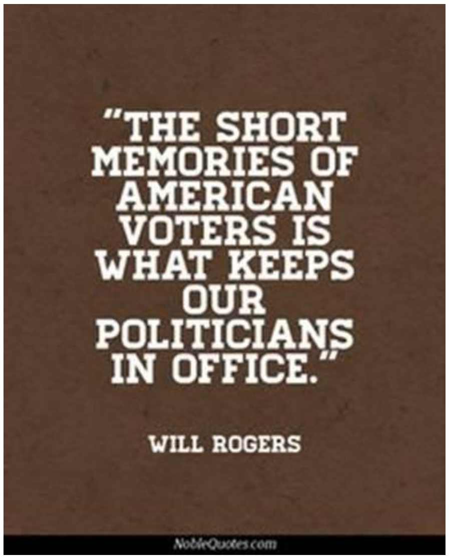
The catch, of course, is that you’ll have to authorize Facebook to access, store, and then match your face data with uploads across the site.

Privacy experts balk at the idea of giving face data to enormous companies like Apple and Facebook, but the social media company has recently moved to further incorporate images of users into their security measures. Throughout 2017, Facebook users have reported being asked by the site for selfies to verify their accounts after suspicious activity was detected. And just last month, Facebook piloted a program in Australia that would essentially block uploads of revenge porn—provided you send the images to Facebook first.

So let’s be clear: Facebook has set up new privacy and security schemes that would guzzle up even more face data. The company should similarly scale up its transparency efforts and be even more forthcoming, particularly if this is being done to protect people from having their photos abused, as Facebook claims.

As part of today’s announcement, Facebook published a blog post titled “Hard Questions: Should I Be Afraid of Face Recognition Technology?” featuring the above video. Neither, however, mentioned the ongoing lawsuit against Facebook over its handling of user’s faceprints. Facebook is currently fighting off a class action suit in Illinois that argues the company violated the state’s Biometric Information Privacy Act. BIPA sets a certain threshold of transparency from companies that collect and store biometric data. Facebook, the suit alleges, doesn’t meet the threshold because it hasn’t full disclosed its intentions.

Thought for the month!



“THE SHORT MEMORIES OF AMERICAN VOTERS IS WHAT KEEPS OUR POLITICIANS IN OFFICE.”

WILL ROGERS

NobleQuotes.com