Member of apcug An International Association of Technology & Computer User Groups

The Rochester Computer Society, Inc.

a computer/tech club open to everyone

MONITOR

Vol. 38, No. 03 Rochester, NY March 2020

Our Club

RCSI is a nonprofit 501(c)(3) group open for membership to anyone interested in computers and related technology. Our aim is to provide an exchange of information between users of digital devices. We are not in any way affiliated with any computer manufacturer or software company.

Program Meetings

No admission fee for non-members*. *Everyone is welcome! Second Tuesday of every month, except August, from 6:30pm – 8:30pm.

Help's Half Hour (Q & A) 6:30pm – 7:00pm. *Members and Guests are welcome to attend and bring their computer related questions with them to get answered.*

7:00 – 7:15, Club Business

7:15 – 8:30+, Main Presentation

Come and join in the fun and enjoy a snack! **You are welcome to bring a guest**.

Become a Member

Go to our website, www.rcsi.org, and download a printed form for use by the Post Office mail, **or** enter your info online and pay with a credit card or PayPal, **or** attend a meeting.

The *Monitor* is published monthly by members of RCSI. Articles by our members may be reprinted by other user groups or nonprofits, without special permission, provided they are unaltered. A courtesy copy may be emailed to our author or Monitor editor.

Tuesday, March 10, 'Browser Bloat & Service Workers: What to do about them?', a Mark Zinzow presentation

Tuesday, April 14, Video Night

selected videos by Tony Dellelo

In This Issue

Wawa Breach: Hackers Put 30 Million Stolen Payment Card Details up for Sale

By Wang We, January 30, 2020

Remember the recent payment card breach at Wawa convenience stores?

If you're among those millions of customers who shopped at any of 850 Wawa stores last year but haven't yet hotlisted your cards, it's high time to take immediate action. That's because hackers have finally put up payment card details of more than 30 million Wawa breach victims on sale at Joker's Stash, one of the largest dark

"Your Computer User Group of the Air", Saturdays from 12:00 pm to 2:00 pm, with Nick Francesco, Dave Enright, and Steve Rae. Broadcasting on JAZZ 90.1 FM (WGMC) from Rochester, NY. Call 966-JAZZ (585-966-5299) or 800-790-0415

Sound Bytes is the longest running computer call-in show in the known universe.

Free copies of the RCSI **'Monitor'** newsletter can be found in the following computer stores: Microworx, TSC Electronics, Pod Computers, and Just Solutions. Digital copies may be obtained from **www.rcsi.org** or my **Pcloud** storage at **https://tinyurl.com/tonydel-rcsi**. Also includes presentation slides and articles too large for this newsletter.

Some Past Presentations:

Cut the Cord, Streaming Services
Autonomous Cars and Robots
Open Source and Free Software
Protecting Your Identity
Keeping Mobile Devices Secure
3D Printing, ENABLE project
Flash Drives-Not Just for Storage
Features, Mac OS X & Windows
Tablets, the Programs and Uses
Personal Finance Software
Amazing Browser Tips
Linux is Like Cars
Drones and Their Many Uses
Gifts and Gadgets for the Holidays

web marketplaces where cybercriminals buy and sell stolen payment card data.

As The Hacker News reported last month, on 10th December, Wawa learned that its point-of-sale servers had malware installed since March 2019, which stole payment details of its customers from potentially all Wawa locations. At that time, the company said it's not aware of how many customers may have been affected in the nine-month-long breach or of any unauthorized use of payment card information as a result of the incident. Now it turns out that the Wawa breach marked itself in the list of largest credit card breaches ever happened in the history of the United States, potentially exposing 30 million sets of payment records.

According to threat intelligence firm Gemini Advisory, on 27th January 2020, hackers started uploading stolen payment card data from Wawa at Joker's Stash marketplace, titled as '**BIGBADABOOM-III**,' which reportedly includes card numbers, expiration dates, and cardholder names. "While the majority of those records were from US banks and were linked to US-based cardholders, some records also linked to cardholders from Latin America, Europe, and several Asian countries," Gemini Advisory said. "Non-US-based cardholders likely fell victim to this breach when traveling to the United States and transacting with Wawa gas stations during the period of exposure." "The median price of US-issued records from this breach is currently $17, with some of the international records priced as high as $210 per card."

In the latest statement released yesterday, Wawa confirmed that the company is aware of reports of criminal attempts to sell customers' payment card data and to help further protect its customers, the company has 'alerted payment card processors, payment card brands and card issuers to heighten fraud monitoring activities.' "We continue to encourage our customers to remain vigilant in reviewing charges on their payment card statements and to promptly report any unauthorized use to the bank or financial institution that issued their payment card by calling the number on the back of the card," Wawa said. Customers who bought anything from any of the Wawa convenience stores between March and December last year are advised to block the affected cards and request a new one from your respective financial institution.

This article was reprinted – *without getting permission* – from www.thehackernews.com/2020/01/wawa-credit-card-breach.html.

[ALERT] Have You Been Smished?

By Bob Rankin, www.askbobrankin.com
a Translator for the Technology Impaired

Spammers and scammers are endlessly adaptable, switching to new attack vectors as rapidly as users catch on to old ones. One of the "new" vectors is actually many years old, but it's achieving some prominence now as mobile phones have become nearly ubiquitous and users have raised their guards against email phishing scams. Read on for the scoop, and how to protect yourself from "smishing" attacks.

Special Interest Group

Linux Sig

We are back!

Linux Workshop,
third Saturday of the month
Sat, March 21, Noon-4PM

NEW LOCATION:
Gates Public Library
902 Elmgrove Rd, 14624,
between Buffalo Road and
531 Expressway.
The room we use is on the second floor, SE corner, by the restrooms.

https://www.meetup.com/Interlock-Rochester-Hackerspace/events/psggnqybccbxb/

Come and get your questions about Linux answered. We have experts on hand to fix problems and answer questions about Linux and FOSS (free and open source software). ***Bring your system in*** so we can help you get the most out of it. Hope to see you there.

Carl Schmidtmann

Free, **Virtual Technology Conferences**, ONLINE
presented by APCUG

remaining 2020 Schedule
Saturdays: May 2, Aug 15, Nov 7
from 1 – 4 pm, EST

For Conference Descriptions & Registration Links, go to
apcug2.org/category/ virtual-tech-conference

What is Smishing?

"Smishing" stands for "SMS phishing." It's a social-engineering technique that relies on text messages to dupe users into taking actions that reveal their sensitive personal information, or lure them to a rogue website that will trick them into handing over a credit card, or sneakily infect their phones with malware.

A smishing message includes the usual elements of a scam: the false appearance of a trusted sender; a message designed to grab your attention; and an urgent call to action that promises a reward or a solution to a problem. You'll have much bigger, real problems if you perform the suggested action.

The action requested may be a voice phone call to "account services" at your bank, Amazon, or another large company that most people know and trust. It may be a demand that you visit a website via a link provided in the message. Less often, it's a request for a reply that leads to a text message dialogue with a scammer, or an automated bot that seems to be a person.

Whatever the action is, it leads to subtle requests for more and more information: Social Security Numbers, addresses, credit/debit card info, login credentials, etc. These are things that no legitimate company will ever ask you to provide or "verify" via text message, email, or over the phone.

Smishing has been around for many years, but recently there has been a surge of smishing attacks that has security experts sounding the alarm more loudly. There are several reasons why smishing is a growing threat:

Why is Smishing a Growing Concern?

This is a good time to remind AskBob readers about the importance of Two-Factor Authentication, or 2FA for short. It sounds geeky, but it's actually a simple tool that can protect you even if a hacker steals all your passwords. See my article What is Two-Factor Authentication? for details on that. And while we're on the subject, see my 5-Point Tuneup For Hacker Defenses.

The response rate of email phishing has fallen considerably, as more users become aware of the telltale signs of phishing and refuse to take the bait. But many people still trust their phones, and are unaware of the techniques that scammers can use. Another factor is that people are often distracted and on the move when they receive a text, and may respond without thinking.

A smishing message might include a warning purportedly from your bank, informing you of an unauthorized purchase, or some other company telling you that your account was frozen due to fraudulent activity. Another common one is the "You just won a prize (or gift card)" message. These scams may encourage you to call a phone number. Don't -- instead call the company (with a phone number you know is correct) and report the message to their security department. Or just chuckle, and delete it.

Recently, text messages that appear to be from FedEx include a tracking number and a request to "set up delivery preferences" for a package that's en route. Of course there's a link to click, which takes the unsuspecting to a page that (drumroll, please...) informs them that

RCSI Officers

Pres: Steve Staub 429-9877
srstaub1@rochester.rr.com
VP: Mark S. Lawson . . . 544-5377
mslawson51@peoplepc.com
Treas: Jerry Seward . . . .
jerry@jerryseward.com
Secretary: www.rcsi.org
Help's Half Hour . . Jan Rothfuss

Board Members at Large

Jan Rothfuss 347-6020
jan_rothfuss@hotmail.com, 9/22
Tony Dellelo 734-6149
tonydel@techie.com, 9/21
Bob Avery 385-4491
webmaster@rcsi.org, 9/20

Standing Committees

Linux SIG: . . . Carl Schmidtmann
unixgeek@faultline.com
Programs and *Monitor* editor: . . . .
. . . . Tony Dellelo
Webmaster: . . . . Bob Avery
Membership: . . . . Steve Staub

Planning Meeting

Held on 1st Tuesday of each month at 7 pm, at St. John's Meadows, Briarwood building. ANY CLUB MEMBER MAY ATTEND.

Newsletter Printing

* ON HOLD AT THIS TIME *

The newsletter was printed at St John's/Chestnut Court by the printing group, with the help of Don Wilder (computer and printer operator). *We will try and print on the 1st or 2nd **Thursday morning** following the monthly meeting.*

Club Address

Rochester Computer Society, Inc
2 Bambi Lane
Rochester, NY 14624

they've won a fabulous prize! All you have to do is complete a survey, and pony up your credit card to cover the shipping fee. That's where things get worse.

FedEx does offer customers the option to sign up for text message alerts about packages they have sent or received. That's why this particular smishing scam has credibility at first glance.

The cost of sending smishing messages is virtually zero, allowing more bad actors to get into the smishing game with ever-higher volumes of bogus messages. Some bad guys run SMS servers that they rent out to other bad guys, making smishing attacks as easy as writing a bogus message and clicking on a few options. These scam-as-a-service operators even provide bogus websites that look very much like those of familiar banks and other trusted companies.

There are no apps that detect smishing messages effectively. It's incumbent upon you to know the telltale signs of a scam and just refuse to go along with it. Never call a phone number in a text that purports to be your bank's. Never click on a shortened URL in a text message; you have no idea where it will lead. Keep your mental guard up at all times.

If you're not sure who the sender of a text message is, my advice is to delete it and move on. Have you ever gotten a suspicious text message, or one that was just spam? Your thoughts on this topic are welcome. Post a comment or question on my website.

# # #

* * * * * SOFTWARE and HARDWARE * * * * *

The Sneaky Simple Malware That Hits Millions of Macs

How the Shlayer Trojan topped the MacOS malware charts—despite its "rather ordinary" methods.

Shlayer's not the most sophisticated malware on the block, but its distribution network makes it surprisingly common on Macs. The popular misconception that Macs don't get viruses has become a lot less popular in recent years, as Apple devices have weathered their fair share of bugs. But it's still surprising that the most prolific malware on macOS—by one count, affecting one in 10 devices—is so relatively crude.

This week, antivirus company Kaspersky detailed the 10 most common threats its MacOS users encountered in 2019. At the top of the list: the Shlayer Trojan, which hit 10 percent of all of the Macs Kaspersky monitors, and accounted for nearly a third of detections overall. It's led the pack since it first arrived in February 2018.

You'd think that such prevalence could only be achieved by comparable sophistication. Not so! "From a technical viewpoint, Shlayer is a rather ordinary piece of malware," Kaspersky wrote in its analysis. In fact, it relies on some of the oldest tricks in the books: convincing people to click on a bad link, then pushing a fake Adobe Flash update. Even the trojan's payload turns out to be ho-hum: garden variety adware.

Tidbits of probably useless information

Canada is the fastest warming country in the world.

The fastest muscles in the human body, are those that make your eyes blink.

Of all the organs in the human body, the tooth is the only one that cannot heal itself.

The human skeleton is renewed every 10 years.

Of all the bones of the body, the femur, located between the hip and the knee, is the most resistant. It can support 30 times its weight, and it is stronger than concrete.

Every human being has a unique tongue print, just like fingerprints, but also the iris of the eye and the shape of the ears. Our language has both geometrically shaped information and unique physiological texture information.

French was the official language of the English court from 1066 to the beginning of the fifteenth century. A few decades later, French became the official language of France in 1539. Before that, Latin was the language of France.

From the fifth century BC, in Antiquity, we shook hands to establish a confidence pact: no one was going to use this hand to take out his weapon. Later, the knight extended his hand to show that he was not going to take his sword out of its sheath.

The Iceland Parliament (930 AD) is the oldest parliament still in operation in the world.

Shlayer's brilliance, it turns out, lies less in its code than its method of distribution. The operators behind the trojan reportedly offer website owners, YouTubers, and Wikipedia editors a cut if they push visitors toward a malicious download. A complicit domain might prompt a phony Flash download, while a shortened or masked link in a YouTube video's description or Wikipedia footnote might initiate the same. Kaspersky says it counted more than 1,000 partner sites distributing Shlayer. One individual, Kaspersky says, currently owns 700 domains that redirect to Shlayer download landing pages.

"Distribution is a vital part of any malware campaign, and Shlayer shows that affiliate networks are pretty effective in this sense," says Vladimir Kuskov, head of advanced threat research and software classification at Kaspersky.

While Shlayer is simple, the adware it installs—a wide variety, since Shlayer itself is just a delivery mechanism—can deploy at least a modestly clever trick or two. In an instance of Cimpli adware that Kaspersky observed, the malware first poses as another program, in this case Any Search. In the background, Cimpli attempts to install a malicious Safari extension, and generates a fake "Installation Complete" notification window to cover up the MacOS security notification that warns you against doing so. It tricks you, in other words, into granting permission to let it run amok on your device.

Once you do, the attacker can both intercept your search queries and seed the results with their own ads. It's an annoyance, more than anything. But given that over 100 million people use MacOS, and it hits at least 10 percent of those with Kaspersky installed, it's reasonable to assume that millions of Mac users deal with it every year. It's not clear how many it actually infects; a thunderstorm drops rain on lots of houses, but only a handful leak. But even if only a small percentage of those attempts prove successful, it's apparently enough to keep the operation going.

"Apple does a great job making their OS more and more secure with every new release," says Kuskov. "But it is hard to prevent such attacks on the OS level, since it's the user who clicks on a link and downloads Shlayer and runs it, like any other software."

While Flash might seem like an outdated lure, given the numerous public warnings about its fallibility and the fact that it's dying off completely this year anyway, it's actually perversely effective.

"I think the reason why fake Flash Players are so successful, in spite of these facts, is twofold," says Joshua Long, chief security analyst at Intego, which first discovered Shlayer nearly two years ago. "Force of habit, and lack of awareness of the current state of Flash."

To the first point, people have been so accustomed to serious Flash vulnerabilities that they're conditioned to update ASAP to avoid calamity. As for the second, Long says, "the average consumer has no idea that Flash is rarely used by modern sites, that Flash installers are no longer necessary, or that Flash is being terminated this year."

None of which means Mac owners are especially susceptible. "The techniques used to deceive users to install Shlayer also work fine with users of any other platform and OS," Kaspersky's Kuskov says.

The best ways to protect yourself from Shlayer and other malware are similarly universal. Don't click suspicious links, especially not surprise

Jere's Tech Tips

By Jere Minich, Apcug Advisor, Region 5 (AL, FL, GA, SC)

WHAT'S THE DIFFERENCE BETWEEN 5G AND 5GHZ WI-FI? – 5G and 5 GHz Wi-Fi are both used for wireless connectivity, but they don't have anything else in common. Anyone referring to "5G Wi-Fi" actually means 5 GHz Wi-Fi, which is different from the 5G cellular standard.

Go to this How-To Geek article and learn the difference between these terms. http://bit.ly/35zYYAu

10 WAYS TO BOOST YOUR WI-FI SIGNAL – Check out these quick tips to boost your wireless signal from your router, extend and optimize your Wi-Fi coverage, and speed up your surfing.

Browsing slowing to a crawl, the inability to stream, dropped Wi-Fi signals, wireless dead zones—every one of these problems is maddening in a world where getting online has become, for some, as necessary as breathing. (Well, maybe not that critical… but important.)

If you feel like your Wi-Fi has gotten sluggish, there are many tools you can use to test the speed of your Internet. However, if the only way you can get decent reception is by standing next to your wireless router, these simple tips can help optimize your network.

Go to this PC magazine article and tune up your Wi-Fi signal. http://bit.ly/2SZPmfQ

pop-up windows. And don't install Flash in the year of our lord 2020—especially not from a site that's promising a pirated livestream.

I found this article at www.wired.com/story/macos-shlayer-trojan-adware.

How living with AI can improve your daily life

(BPT) - These days, AI - artificial intelligence - has become a household name, mostly because so many household gadgets and appliances use it.

What's the impact of AI becoming part of your everyday life? Ultimately, it's about convenience. Many tasks are getting easier, products are more efficient and AI is enhancing daily lives in unexpected ways. Here are some recent AI advances that may be improving your life.

Appliances that can think and learn

You may not have expected laundry machines to be among the major appliances to use AI, but it's true - the latest innovations in washers and dryers allow consumers more freedom in controlling their machines, and help those machines apply more precision in how they handle different types of clothing.

For example, LG Electronics introduced an AI-powered TurboWash 360 Front-Load Washer/Dryer Pair. The Ultra Large-Capacity washer assesses fabric type, weight and softness to choose the best washing motions for a superb clean. The advanced spinning algorithm measures load size to minimize vibrations, noise and spin time. LG's user-friendly ezDispense feature takes the guesswork out of detergent dosage by automatically adding the exact amount of detergent and fabric softener needed for each load.

Because the washer and dryer both utilize AI to learn from usage patterns over time, settings continually optimize for the best results. The machines are also Wi-Fi connected, so you can control the units or monitor cycle times remotely using ThinQ-enabled smartphones or voice commands via Amazon Alexa. When the washer is synced with your Amazon account, it can reorder detergent before you run out.

Enhanced entertainment platforms

Just a few years ago, TVs couldn't perform half the functions they can today. Using ThinQ AI and powered by the α (Alpha) 9 Gen 3 AI processor, the latest LG OLED TVs bring picture and sound quality to a whole new level - and are used for much more than watching shows.

These TVs apply a deep learning algorithm to recognize content source quality, then determine the best method for optimal picture quality among four genres: movie, sports, standard and animation. The new processor finely adjusts the picture, taking into account the room's ambient conditions to offer the best levels of screen brightness and contrast, using its understanding of how the human eye perceives images. What's more, the processor's AI Picture Pro is capable of recognizing faces and text on screen, fine-tuning and sharpening each to

Programs recommended by our members

ANTI VIRUS

How does **Avira Free Antivirus** compare to Avast Free Antivirus? Both products are very similar and offer great sets of features. However, Avira is scoring lately as **#1 antivirus** in the independent tests, especially in the virus and malware detection and a low number of false positives.

On the other hand, Avira is much more aggressive in terms of up-selling to paid versions and the pop-up offers are extremely annoying. Of course, Avast is using them too, but not that frequently.

Avira has also recently started pushing a new product called **Avira Free Security Suite**, which combines all Avira free products – Antivirus, Phantom VPN (500 MB/month), Password Manager, System Speedup, Scout (browser) and Software Updater. Obviously, the whole free suite requires much more system resources, so we recommend staying with the basic Free Antivirus and adding the components you need.

Avast definitely offers more in terms of advanced features and tools like Home Network Security for scanning router vulnerabilities, Browser Cleanup for scanning browser extensions, or Software Updater for scanning outdated software in your system. Avira is purely an antivirus, which isn't necessarily a bad thing. Both products offer an option to create a bootable disc, with the latest antivirus version to clean your system when it doesn't start.

produce more natural skin tones, well-defined facial features and clearer, more readable characters.

Even sound is enhanced by the intelligent algorithm, which can mix two-channel audio to deliver convincing surround sound. Thanks to LG's AI Sound Pro, LG OLED TVs analyze and classify the audio of content among five categories - music, movies, sports, drama or news - for clearer voices and richer, more textured background sound.

The latest lineup of TVs also matches perfectly with LG's stylish 2020 sound bars, which are future-proofed to help you create seamless visual harmony in any room. These advanced models are self-calibrating, able to recognize and analyze tones to accurately assess the dimensions of a given space and adjust accordingly.

With ThinQ and a built-in connection to Google Assistant and Alexa Amazon, you can use your TV to control other compatible devices and appliances, search the web - and even order pizza without pausing the movie you're watching!

Advanced mobile communication

What could be better than experiencing LG OLED TV technology in your home? How about holding it in your hand? Using LG's latest LG V50 ThinQ 5G smartphone, you can enjoy LG OLED quality display on demand, with striking clarity and vibrant color. The ability to communicate, record and enjoy pictures and videos, plus livestreaming shows and movies on-the-go has reached new levels of speed and quality, especially with the revolutionary new 5G connectivity. You can also use its five cameras to create and share high-quality content. With three rear cameras and two front cameras, you can capture truly original selfies, pictures and videos with rich detail.

Artificial intelligence may still sound like science fiction, but the truth is, everyone is using it more and more each day. AI technology is helping people perform tasks and enhancing everyday life in so many ways - and there's no telling what the future may bring.

Customers can add this new feature by accessing the LG support and updating their compatible TV's firmware with the latest version posted on that support site. TV models and release dates may vary by region.

From the Brandpoint website,
www.brandpointcontent.com/article/35510/how-living-with-ai-can-improve-your-daily-life.

My Experience with a subscriber VPN

Advantages, costs, pitfalls, workarounds Part 1 of a 2-part article series

Author: John Krout, Member
Potomac Area Technology and Computer Society (PATACS)

This article is based on a lot of research, several years of use of a corporate VPN at work, and a few months of using a subscriber VPN at home.

Some Interesting Websites and Internet Finds

THE MOST POPULAR HEALTH WEBSITES

WebMD, top-notch advice and a reference used by many doctors, www.webmd.com

NIH, National Institutes of Health, www.nih.gov

Yahoo Health, www.yahoo.com/lifestyle/tagged/health

Mayo Clinic, Rochester, MN, www.mayoclinic.org

MedicineNet, www.medicinenet.com/script/main/hp.asp

Drugs, with interaction checker, www.drugs.com

Everyday Health, www.everydayhealth.com

Health Grades, find the right doctor, www.healthgrades.com

Healthline, www.healthline.com

Mercola, take control of your health, by Dr Joseph Mercola, a New York Times best selling author, www.mercola.com

Health, delivers relevant information in clear, jargon-free language that puts health into context in peoples' lives, www.health.com

MindBodyGreen, here you'll find a 360-degree approach to wellness that weaves the mental, physical, spiritual, emotional, and environmental aspects of well-being together, www.mindbodygreen.com

VPN is an acronym for Virtual Private Network. The idea is that your use of a VPN provides a secure method of data communication, through strong encryption. The encryption hides the info in your communication, such as content of emails and URLs of web sites, from your Internet Service Provider (ISP) and any other **Man in the Middle**.

WHY VPNS EXIST

That phrase Man in the Middle is important. Your communication with your email server or any Web site may pass through half a dozen or more servers in between. For any one of those in-between servers, any bored or underpaid system administrator, and any hacker breaking in, might install message trapping software to capture info passing through, such as your IDs and passwords for your stockbroker or bank. Those snooping activities are called Man in the Middle attacks. Encryption makes it almost impossible for them to make use of that info.

Originally, when local area networks (LANs) first became available, the only networks were inside a single building where all the computers were connected on the local network, with no connection to anything outside the building. Later, secure direct circuits, and modems, allowed communication between computers on the inside and the outside.

A very entertaining book, **The Cuckoo's Egg**, written by Clifford Stoll, describes the Bad Old Days before VPNs, when networks were insecure. It is a fascinating read. The author, an astronomer, was given the task of tracking down a 75-cent discrepancy in billing for use of a university local area network. His investigation led him to identify peoples who broke into the network. He found the same people also broke into military computers. He tracked the people to Europe, where they were tried and convicted based on his testimony and a huge pile of printed computer logs as physical documentary evidence. Stoll was a good guy in the middle.

Because of experiences like that, corporations and the federal government have used their own VPNs for many years. VPNs have enabled greater automated data movement, ensuring privacy of the data due to the use of strong encryption. And, now, VPNs are available to the rest of us.

While using a VPN, the encryption is based on two *digital certificates*. The VPN server provides one to your computer, tablet, and smart phone. Additionally, the VPN server itself has another one. The encryption using those two certificates is based on some very creative research done in the early 1980s by three MIT professors, Rivest, Shamir and Adelman, who founded RSA and Verisign, two companies now at the heart of modern digital security efforts.

A second result of the two-certificate approach is that your account is known to be valid by the VPN server, and the VPN server is known to you to be valid as well. Without using a VPN, web sites and other Internet services get access to the Internet protocol address (IP address) of your home router, computer, phone or tablet. This is important because those IP addresses let web sites figure out where you are located. When you use a VPN, the web sites see only the IP address of the VPN server. In this way, a VPN server acts as your proxy, and are sometimes called **Proxy servers**.

Penguin Platform

By “Free John” Kennedy, Apcug Advisor, Regions 3 and 6/7

HOW TO UPGRADE FROM WINDOWS 7 TO LINUX – If you’re still using Windows 7 because you just don’t like Windows 10, that’s understandable. But there’s an alternative upgrade path: You can install Linux on your PC for free, and you’ll have a supported operating system that’s still getting updates.

This is easier than you might think. You can try Linux on your PC before installing it, and you can even install it alongside Windows 7 when you make the leap. Here’s what you need to know.

Read this How-To Geek article for details, with screenshots http://bit.ly/38Cs3NB

DESKTOP LINUX 101: HOW TO EASILY BACKUP AND RESTORE YOUR IMPORTANT DATA – You don’t have to be an avid distro hopper to appreciate the need for a simple and reliable “set it and forget it” backup solution. Desktop Linux provides an array of options on this front, but I’ve found a little utility called Deja Dup to be the easiest by far. So here’s a step-by-step text and video guide, found in Forbes, detailing how to easily backup and restore your important data and documents. http://bit.ly/2L8QGIE

Take a look at **Illustration 1(see note at end of article)**. This shows how a VPN server fits in the overall path of servers between your computer, phone or tablet and the world of the Internet. Inevitably, your VPN-encrypted communications pass through your ISP servers, and then possibly through other intermediary servers until it reaches the VPN server. Using a VPN server severely limits any snooping not only by your ISP but also by any servers between the ISP servers and your VPN server. So the Man in the Middle is stymied in that part of the path.

Beyond the VPN server, the communication is unencrypted by the VPN, or *in the clear*, and at that point reaches the destination, which might be for instance a video streaming server, or a credit card company's web server. Of course, that leg of the path also involves intermediate servers.

Because that leg of the overall communications path is not depicted as encrypted, you might think that a Man in the Middle attack would succeed there.

However, these days most of those destination servers use HTTP-Secure protocol (https), which also employs encryption done in a different way, by your Web browser and by the destination server. That's right, a second encryption. As a result, the communication remains secure all the way through the entire path.

But I want to digress for a moment and suggest that your ISP might also behave as a Man in the Middle.

When you use a VPN, the fact that the servers of your ISP see only encrypted data is very significant. Your ISP is always in the best position to snoop, effectively a Man in the Middle for all the web sites you browse, the streaming services you use, and so forth. All of your browsing and other use of the Internet goes through those ISP servers.

Your ISP has a strong economic incentive to take advantage of that best position: data on the web sites you visit and the downloads you select can be quite valuable to third parties. And don’t think ISPs will ignore that incentive simply because you are a customer of the ISP; the big ISPs convinced the FCC to eliminate Net Neutrality rules so that the ISPs could solicit money from the likes of Netflix and CNN to accelerate delivery of those sites to your computer. So use of a VPN consistently protects you from snooping by your ISP.

MORE ADVANTAGES OF A VPN

I have been using a VPN and HTTPS from my work site for more than a decade. I have seen no significant impact on communications speed. Computers do the encryption and decryption quite quickly these days.

An advantage of subscriber VPN services is that you have access to hundreds or thousands of VPN servers, in many cases spread around the world. If one is busy or down, you can easily use another. Redundancy is a very valuable advantage.

Another advantage is that you can choose a VPN server located in a country where a local web site or video streaming service is of interest to you. For instance, the BBC streaming service is open only to users located in the UK. When the BBC servers detect a request from a US IP address, the servers ignore it. If you use a VPN Proxy server in the UK,

* * Computer Jokes * *
Stolen from Everywhere

Old Timer's Views on Computing

Memory was something you lost with age
An application was for employment
A program was a TV show
A cursor used profanity
A keyboard was a piano
A web was a spider's home
A virus was the flu
A hard drive was a long trip on the road
A mouse pad was where a mouse lived

They Said I Couldn't Break It

About a year ago, Jason, the company's top computer engineer, was called out to make a field service. When he got to the lady's house and was let in, the first thing he noticed was the smell of gunpowder. The second thing he saw was the double barrelled 12-gauge shotgun lying across her lap. And the third thing was the big gaping hole in her computer screen.

Jason looked at her. She was a little grey haired woman, around 60 or so. Had she? Not possible. Still, he had to ask.

Jason: 'Did you shoot...?'

Little Old Lady: 'Yes, I got a little mad at the computer, the program would not load. Tech Support told me that I couldn't hurt it, but I think they were wrong.

Can you salvage anything?'

the UK IP address of the VPN Proxy server tells the BBC that you are local, and you then get to use that streaming service.

A third advantage is far less clear. According to PC Magazine, many VPN users in the US subscribe specifically because the federal government has eliminated the Net Neutrality rules. The idea is the ISP cannot throttle back what it cannot decrypt, meaning what it cannot recognize. NordVPN, for one example, actively promotes that idea on their company's web site. I am not convinced that idea is correct.

COUNT YOUR VPN-READY DEVICES

Another advantage is that subscriber VPN services let you connect more than one of your devices (computer, phone, tablet) to the VPN *at the same time*. This is important if you use two or more Internet-connected devices, like I do. And it is a major convenience factor, allowing you to leave all your devices connected all the time, not just when you actively use each one.

Snoopers can monitor the web browser on your phone or tablet just as readily as they can on your computer. A VPN can and should protect all of those devices.

Several VPN services that I reviewed set a ceiling on the number of concurrent uses by a single account, and that limit varies from 3 to 10.

Because of that, before you select a VPN service, you need to make a realistic assessment of the number of concurrent connections you may need. For example, in my case: I have two Windows computers, two Android tablets, and one Android smart phone, a total of five devices. My son has a Windows computer, a Linux computer, one Android tablet, and one Android smart phone, a total of four devices. So our grand total is nine.

COMPARISON SHOPPING FOR VPNS

When I was shopping for a VPN service, I came across a review of public subscriber VPNs on **TechRadar.com**, published in March 2019. **Illustration 2 (see note at end of article)** is a table comparing the top three VPN services according to TechRadar's ratings system, and some details about them. The number of servers and countries will likely continue to grow for each of the public subscriber VPNs.

The column labeled ceiling of devices per account indicates the ceiling on the number of computers, tablets, and smart phones on which you run the VPN client software simultaneously.

The column labeled # proxy servers is especially valuable for redundancy purposes. If one VPN proxy server happens to be down, or malfunctioning, then you can try many others. Generally, more is better.

Concerning the number of countries, although the overall situation worldwide is improving all the time, to some extent I think there are diminishing returns beyond about 50 countries. This is because smaller countries have fewer localized streaming services, and often do not have high bandwidth connections to the internet, so VPN servers in many smaller cannot work as rapidly as VPN servers in say the US or Canada or western Europe or Japan or South Korea.

Odds and Ends

Linux/Unix Tutorial for Beginners: Learn Online in 7 days

Training Summary

Linux is the most popular server OS. Linux is a clone of UNIX. Knowing one is as good as knowing the other. In this tutorial series, we will be using Linux, as it's freely available. The training will require you to execute certain commands. Make sure to practice them!

What should I know?

Nothing. This tutorial is an absolute beginner's guide to Linux. You don't even have to buy a new PC to learn Linux. You can run Linux, right within your existing Windows or Mac OS systems! (Detailed steps are given in tutorials).

Below, is a taste of the FREE course.

Linux Fundamentals

Tutorial	Introduction to the Linux Operating System
Tutorial	Linux Distributions & Installation
Tutorial	Linux Vs. Windows
Tutorial	Terminal V/s File Manager

Getting Started

Tutorial	Must Know Linux/Unix Commands
Tutorial	File Permissions in Linux/Unix

Continue the course at www.guru99.com/unix-linux-tutorial.html

I chose to subscribe to the **IPvanish VPN service**. Its ceiling on the number of concurrent connections is 10.That was the most important factor for me.

Later on, I found that VPN services are now so popular that PC Magazine reviews the services and provides Editor's Choice awards, their long-coveted recommendation. In 2019, the Editor's Choice awards went to three VPN services:

- TunnelBear (www.tunnelbear.com),
- Private Internet Access (www.privateinternetaccess.com),
- NordVPN (www.nordvpn.com).

NordVPN was the one service that was top rated by both TechRadar and PC Magazine.

PRICING

The VPN services have a monthly rate, usually less than $10, and offer discounts if you pay in advance for say 3 months or for a year. Some even offer further discounts if you pay in advance for three years.

Some VPN services have their business offices outside of the US and may charge your credit card to a bank outside of the US. You may wish to let your credit card company know in advance, so that the charges are not automatically blocked by your card company.

This ends Part 1. In Part 2, you will learn about some difficulties encountered on VPNs, and some workarounds.

ABOUT THE AUTHOR: John Krout is a former president of the Washington Area Computer User Group (WAC), one of two groups that merged to become the Potomac Area Technology and Computer Society (PATACS). He has been writing about personal computer uses since he joined WAC in the early 1980s. He is a frequent contributor to PATACS Posts, and occasionally provides presentations on tech issues at PATACS meetings. He lives in Arlington VA and is a writer for the Thales Group, a major maker of automated fingerprint identification hardware, supporting the use of that hardware in the computer system of a major federal government agency.

From the www.patacs.org, jkrout75@yahoo.com.

Editors' Note: The two illustrations for this article are oversize and would not properly fit on the page. The illustrations can be found on the last page of the web version of this newsletter. www.rcsi.org

* * * * * BITS and PIECES in the NEWS * * * * *

Editor's Note: To continue reading the following articles, you may copy the long URL at the end of the article and enter it into a web browser **or** go to www.rcsi.org/newsletr.htm and click on the URL in the web version of the newsletter.

Handheld 3D Skin Printer Demonstrates Accelerated Healing of Large, Severe Burns

By Eric HamiltonFeb 05, 2020, University of Toronto

A new handheld 3D printer can deposit sheets of skin to cover large burn wounds - and its "bio ink" can accelerate the healing process.

The device, developed by a team of researchers from the University of Toronto Engineering and Sunnybrook Hospital, covers wounds with a uniform sheet of biomaterial, stripe by stripe.

The bio ink dispensed by the roller is composed of mesenchymal stroma cells (MSCs) -- stem cells that differentiate into specialized cell types depending on their environment. In this case, the MSC material promotes skin regeneration and reduces scarring.

The project is led by PhD candidate Richard Cheng, under the supervision of Professor Axel Guenther, and in close collaboration with Dr. Marc Jeschke, director of the Ross Tilley Burn Centre, and his team at Sunnybrook Hospital. Their successful in-vivo trials on full-thickness wounds are reported in the journal *Biofabrication*.

The paper is a major step forward for the team, which unveiled the first prototype of the skin printer in 2018. The device was believed to be the first device of its kind to form tissue in situ, depositing and setting in place in two minutes or less.

Continue reading this article and view a picture of the printer at http://www.sciencetimes.com/articles/24859/20200205/handheld-3d-skin-printer-demonstrates-accelerated-healing-of-large-severe-burns.htm.

India will launch a humanoid robot ahead of its first crewed space mission

Before sending its first crewed mission in late 2021, India will launch a humanoid robot called Vyommitra into space, reports *The Tribune*. It will take flight later this year and in 2021. According to the publication, the robot's name is a combination of the Sanskrit words for "space" and "friend," and as you can see from the video below, the Indian Space Research Organisation (ISRO) modeled it after a human woman -- though it doesn't feature any legs.

The robot told reporters it can operate switch panels, talk to astronauts and monitor a spacecraft's environmental and life support systems. Its primary purpose, however, is to allow ISRO to test how space flight affects the human body before the agency sends astronauts up in one of its Gaganyaan craft.

"It will be simulating exactly the human functions there [in space]. It will check whether the system is right. This will be very useful to simulate, as if a human is flying," ISRO chairman K Sivan told reporters at the media event where the agency showed off the robot.

Finish reading and view the video at www.engadget.com.

Information theft via manipulating screen brightness in air-gapped computers

by Nancy Cohen , February 8, 2020, Tech Xplore

Data can be stolen from an air gapped personal computer just by using variations in screen brightness. Researchers at Ben-Gurion University wrote a paper on it.

As the team defines them, "Air-gapped computers are systems that are kept isolated from the Internet since they store or process sensitive information."

That they have come up with yet another discovery on how to wrest sensitive data from a computer came as no shock to *Naked Security*, which recognized that "Researchers at Ben-Gurion University of the Negev have made a name for themselves figuring out how to get data out of air-gapped computers. They've dreamed up ways to communicate using speakers, blinking LEDs in PCs, infrared lights in surveillance cameras, and even computer fans."

Graham Cluley writing in *Tripwire* reckoned, ok, "It may not be the most efficient way to steal data from an organisation, let alone the most practical, but researchers at Ben-Gurion University in Israel have once again detailed an imaginative way to exfiltrate information from an air-gapped computer."

Wow, continue at www.techxplore.com/news/2020-02-theft-screen-brightness-air-gapped.html.

* * * * * CLUB and REGIONAL NEWS * * * * *

Imagine RIT 2020, Saturday, April 25 **About the Festival**

Imagine RIT: Creativity and Innovation Festival is a campus-wide event that showcases the creative and innovative spirit of RIT students, faculty, and staff. Visitors experience the breadth and depth of RIT through interactive presentations, hands-on demonstrations, exhibitions, and research projects set up throughout campus. Multiple performance stages with live music and entertainment are also a hit with visitors of all ages. Held annually each spring, Imagine RIT is the kickoff to Rochester's rich festival season.

Date & Time: Saturday, April 25, 2020, from 10am to 5pm, ***rain or shine***.

Cost: Free and open to the public!

Location: Imagine RIT takes place throughout RIT's campus in Henrietta, NY

Help's Half Hour

Notes by Jan Rothfuss

Q: Windows 8.1 is restarting very slowly. Another member said he has that issue with 7.0, too. Can take 4 – 5 minutes.
A: Over time, updates can cause the system to be overloaded. Be sure you are running protective programs like SuperAntiSpyware, MalwareBytes etc.

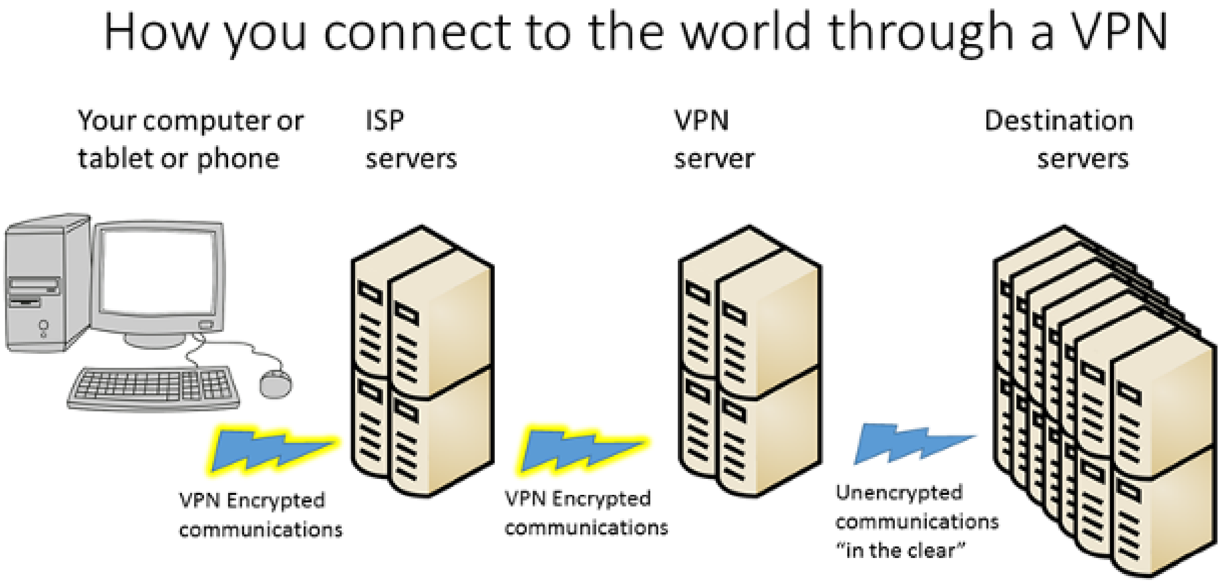
Q: A friend has a Hotmail account but is now getting a message that he must reset it.
A: He may have to go to Microsoft

We live in a wonderful age, the 'Age of the Internet'. If you have a computer question, you can 'google' it and usually get the solution in a moment or two. BUT, we need questions for our 'Help's Half Hour' section, so how about a compromise. Bring a question to the meeting and share the solution with the members.

Our Meeting Place

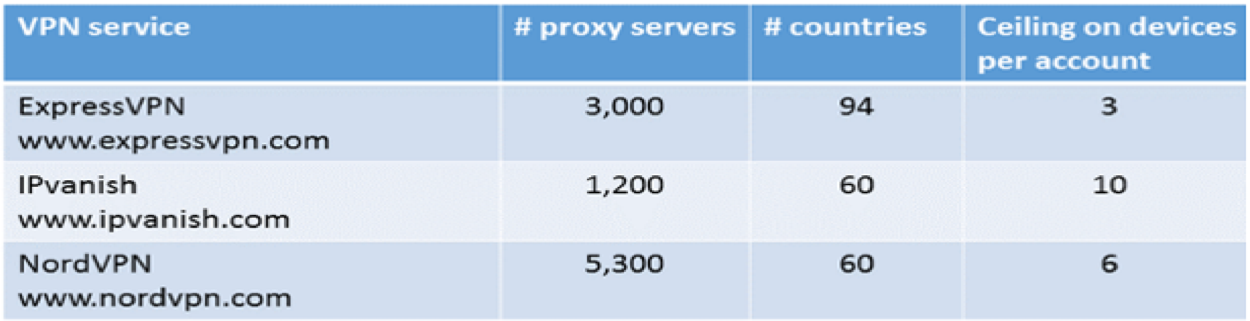
St John's Meadows at Johnsarbor Drive, is on the left, past Clinton Avenue, when going West on Elmwood Avenue. The opening in the white fence is Johnsarbor Drive. At the 'T', turn right. The meeting is in the first building on the left – **Briarwood**.

Our meeting place can change. Please check our website before each meeting. **www.rcsi.org**


How you connect to the world through a VPN

Your computer or tablet or phone
ISP servers
VPN server
Destination servers
VPN Encrypted communications
VPN Encrypted communications
Unencrypted communications "in the clear"

Illustration 1.



VPN service	# proxy servers	# countries	Ceiling on devices per account
ExpressVPN www.expressvpn.com	3,000	94	3
IPvanish www.ipvanish.com	1,200	60	10
NordVPN www.nordvpn.com	5,300	60	6

Illustration 2.