SUPERCOM COMPUTER CLUB TECH TIMES

Volume 15 September 25, 2017

Objective:

To bring the latest technology news to you, our members. Tips and suggestions will help you to keep your device(s) running smoothly and help you be aware of threats. Technical tips will be coming to you through our Technical Committee.

Committee Members: (Pictured Below)

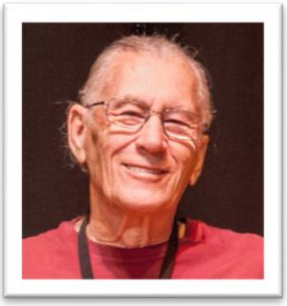
Ben Tarbell, Mike Gerkin, Jim Oliver, Peggy Bullock, Jim Mills, Rick Heesen, Lowell Lee, Steve Andreasen (Apple/Mac), Dick Strong and Art Rice.



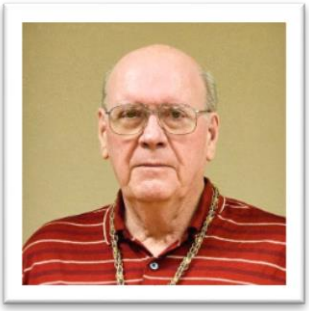








Dick Strong is on “time off” for season 2016-2017.



Greetings

Think you have to put your glasses on because you just received an email notice that there is another Tech Times posted on the website? Well, you don't need them to know that is true, but you may need them to read the latest information. Seems we have some major breaches in our technological world and we have to keep up with them. So, be sure to read the latest news from our members!!

****

Submitted by Mike Gerkin:

We are sure by now all of you have heard and discussed the hack of Equifax which now has grown into an even larger breach of security. This article from *Ask Leo* leads to one of the better commentaries on the seriousness and potential risk of the major incident.

What the Equifax Breach Means to You

On September 7th, the U.S. credit reporting company Equifax announced they had suffered a massive data breach some months earlier.

Equifax's handling of that breach has since been termed a "dumpster fire" by noted journalist Brian Krebs. Their instructions, website, and tools to help you determine if you've been impacted have been nothing short of a total mess. The term I'd use instead of dumpster fire isn't appropriate for a family publication.

All indications are that if you've ever had a credit report, your information is likely part of this mess. Even if you're not sure, it's best to assume it.

So. What now?

It's not about passwords

Most of the breaches I discuss are serious because they include account IDs and (hopefully hashed) passwords. The theory is that attackers could use that information to access your existing accounts.

When that's the case, the general advice is to change the passwords on any affected accounts and make sure that you're not using the same password on multiple accounts.

While the latter is always important advice (even when you're not the subject of a breach), changing your passwords won't help in this case.

Passwords weren't involved.

It's about personal information

The stolen information is said to include:

- Names
- Social Security numbers
- Birthdates
- Addresses
- Driver's license numbers

In addition, some people had their credit card numbers and credit report dispute documents (which include personal identifying information) stolen as well.

The hackers apparently have had access to all this information for a couple of months.

Why this is bad, very bad

Two words: identity theft.

Consider just the first four items in the list above: names, Social Security numbers, birthdates, and addresses. That's generally enough to open a credit card account in your name — a credit card account hackers could use and that the credit card company will think is your responsibility.

There are more scenarios beyond just credit cards. Most probably involve getting credit or loans in your name without your consent or knowledge. You are then faced with having to contest those charges, and may have trouble using your credit legitimately, since the hackers will have tarnished your good reputation in the eyes of banks and creditors.

What you can do next

The single most important thing you can do is *simply pay attention*. Pay attention to your bills, credit cards, paper junk mail, and to what looks like spam that lands in your inbox.

Watch all your monthly bills for unexpected charges. This isn't limited to credit cards, but any charge for which you are notified via paper or electronic mail. If they're not legitimate, contact the company *immediately*.

Monitor your credit cards closely. In my opinion, simply reviewing the paper statement once a month isn't enough. I enable online access and check more frequently — every few days or at least once a week. In addition, I use credit card services that notify me by text or email each time a charge over a certain amount is made. If I can, I set it to any charge over $1, so I know exactly what's happening. If you see something suspicious, contact the credit card company *immediately*.

Open the junk mail in your physical mailbox. Often the first notification that something is amiss is a statement or welcome letter from an account you've never heard of. You've never heard of it because you didn't open it — the identity thief did. If it looks like someone opened an account in your name you did not authorize, contact the company *immediately*.

Watch the spam that lands in your inbox (#1). What you think is spam, because it's about a company or an account you don't have, could potentially be “legitimate” in that it's actually from the company mentioned, and you do have an account with them … an account opened by an identity thief. If you suspect that's the case then contact the company *immediately*.

Watch the spam that lands in your inbox (#2). Phishing attempts are likely to be on the rise. Using the stolen information, hackers craft even more convincing (yet fake) emails trying to get you to fall for their schemes. Pay extra close attention to all email that leads you to log into your bank, credit card company, or any other website that deals with your personal information. Never click on the link to those sites in email, but instead go to those sites using your own links and bookmarks.

If you find you are the victim of identity theft, even for just a single account, it's important to contact law enforcement as well. Many of the remedies and mitigations rely on police or other formal report being filed.

What you might consider

Part of the mess that is Equifax's handling of this situation revolves around a tool on their website set up to help people determine whether or not they are impacted by the breach. As I write this, it's poorly constructed and exceptionally uninformative. I honestly can't recommend using it just yet.

The traditional response to identity theft is to set up a credit lock or credit monitor on your credit reports. It's a hassle you have to do yourself with each of the three major credit reporting companies: Equifax, TransUnion, and Experian. There are two problems:

1. How can we trust Equifax to get it right, in light of this massive breach?
2. Depending on where you live, it may or may not be free. In my state (Washington), I'm required to actually *be* a victim of identity theft, with a corresponding police report to prove it.

I have to admit I'm seriously considering it anyway. I'm also paying attention to any activity on any of the free credit reporting sites, such as Credit Karma. (**Important**: there are many misleading “free credit report” sites out there. The official site to get your free annual credit reports, as confirmed by the FTC, is annualcreditreport.com.)

An alternative is a more restrictive credit freeze, which is something embraced by Brian Krebs, and something I'm now also considering.

Stay Alert

As I said above, it's important to pay attention to what's happening to your money and your credit. With random threats, breaches, and hacks happening periodically, that's good advice even without the Equifax mess.

More details about the Equifax breach will no doubt come to light in the coming days, hopefully along with more concrete ways to determine if you're impacted. Keep your eyes on the news and other information sources to keep up-to-date.

Updates

2017-09-14: I did end up freezing my credit with Equifax and Experian, and signing up for the free tier of TransUnion's “TrueIdentity”, which also allows you to “lock” access to your credit profile. The process was not painful, and all accomplished online. Equifax was free, having removed the fee for a credit lock until the end of the month at least, and I paid Experian $11 (the fee is based on what state

you live in). If you freeze your credit: **DO NOT LOSE THE PIN** you're assigned. Seriously, I can't overstate the importance of having that PIN should you need to unlock your credit for any reason.

2017-09-14 #2: I also just received my first spam mentioning the Equifax breach specifically. It's likely a phishing attempt in the guise of a free credit report offer. *Never respond to or act on unsolicited requests* like that. They are almost certainly bogus. Instead, go to known resources — such as those I've listed above — yourself.

https://newsletter.askleo.com/ask-leo-670-equifax-breach-means/

****

Submitted by Peggy Bullock:

The following article from Kim Komando also addresses the Equifax breach and is very well written with some tips to follow:

Most likely, you or someone you know has been negatively affected by the Equifax data breach. That's because 143 million, nearly half of all Americans, had sensitive data stolen in the breach. Yikes!

We've already given you important steps that you need complete following this massive breach. However, there is one more thing that everyone needs to do to secure their Social Security number. Click the share button located on the left side of this article to post it on Facebook, it's critical that your friends and family know this information as well.

How to protect your Social Security number

The Equifax data breach is one of the worst of all time. Critical information stolen includes Social Security numbers, birth dates, addresses, and some driver's license and credit card numbers.

With so many people impacted, the Social Security Administration (SSA) is advising everyone to take the following steps to protect their Social Security number.

Open your personal *my* Social Security account

A *my* Social Security account is your gateway to many SSA online services. Creating your account today will take away the risk of someone else trying to create one in your name, even if they obtain your Social Security number. Follow these instructions to open your account:

- Click here to visit the *my* Social Security account home page
- Click the green tab that says Sign In or Create an Account
- Click the Create An Account button
- Scroll through the terms of service, click on the I agree to the Terms of Service button
- Click Next
- You will be taken to a Please tell us who you are page. Fill this information out and click Next. (You may add an extra level of security to your account. Select yes or no, maybe later.)

- Answer the security questions (These can be tricky, if you get some wrong, your electronic access will be suspended for 24 hours. If your account gets suspended, you can call 1-800-772-1213 and ask for the Help Desk for assistance with your account.)
- Select a username and password

Once you've completed the previous steps, your account has been created.

If you already have a *my* Social Security account but haven't signed in lately, take a moment to log in to take advantage of SSA's second method to identify you each time you log in. This is in addition to the first layer of security, a username and password. You can choose either your cellphone number or your email address as your second identification method.

Using two ways to identify you when you sign on will help protect your account from unauthorized use and potential identity theft. If you suspect identity theft, report it to the Office of the Inspector General and visit identitytheft.gov.

One important note you should know: If you haven't gotten your free annual credit report in a while, now's a great time to do that too. There are many sites that promise you the report for free and then sign you up for other things. Click here to go to the site that really gives your annual credit report for free

What to do if your Social Security number has been compromised

If you know your Social Security information has been compromised, and if you don't want to do business with Social Security online, you can use the Block Electronic Access feature. You can block any automated telephone and electronic access to your Social Security record.

No one, including you, will be able to see or change your personal information on the internet or through the SSA automated telephone service. If you block access to your record and then change your mind in the future, you can contact Social Security and ask to unblock it after you prove your identity. This resource is available to certain victims of identity theft and those who need extra security.

As we said, the Equifax breach is one of the worst of all time. It's very important that you take every precaution to keep your critical data safe. Keep checking in with our Happening Now section for further updates.

Update: We have received email from people who say that you cannot do these steps online if you use a service like Lifelock or have already frozen your credit. You will need to go to a local Social Security Administration office to complete the steps above.

****

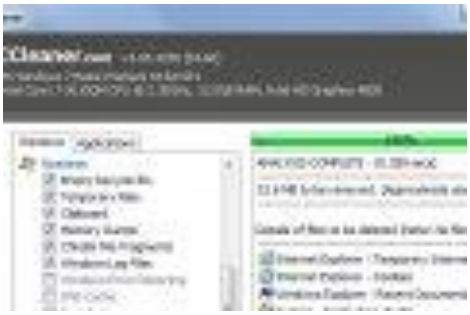
Submitted by Rick Heesen:

CCleaner Was Hacked: What You Need to Know

by **Whitson Gordon** on September 18th, 2017

CCleaner, the incredibly popular PC maintenance utility, has been hacked to include malware. Here's how to tell if you were affected, and what you should do.

RELATED ARTICLE



What Does CCleaner Do, and Should You Use It?

The attack was described thusly by researchers at Cisco Talos: "the legitimate signed version of CCleaner 5.33. . .also contained a multi-stage malware payload that rode on top of the installation of CCleaner." CCleaner's parent company, Piriform (who was recently bought by terrible antivirus company Avast), acknowledged the issue shortly thereafter.

Since CCleaner claims to have millions of downloads per week that is potentially a severe issue.

What Does the Malware Do?

The malware did not actively harm systems, but it did encrypt and collect information that could be used to harm your system in the future. In particular, according to Piriform, it created a unique identifier for the computer and collected:

- Name of the computer
- List of installed software, including Windows updates
- List of running processes
- MAC addresses of first three network adapters
- Additional information whether the process is running with administrator privileges, whether it is a 64-bit system, etc.

You can read more technical info about the attack at Cisco Talos' blog and at Piriform's blog.

Was I Affected?

Thankfully, it looks like this malware only affected a certain subset of CCleaner users. In particular, it affected:

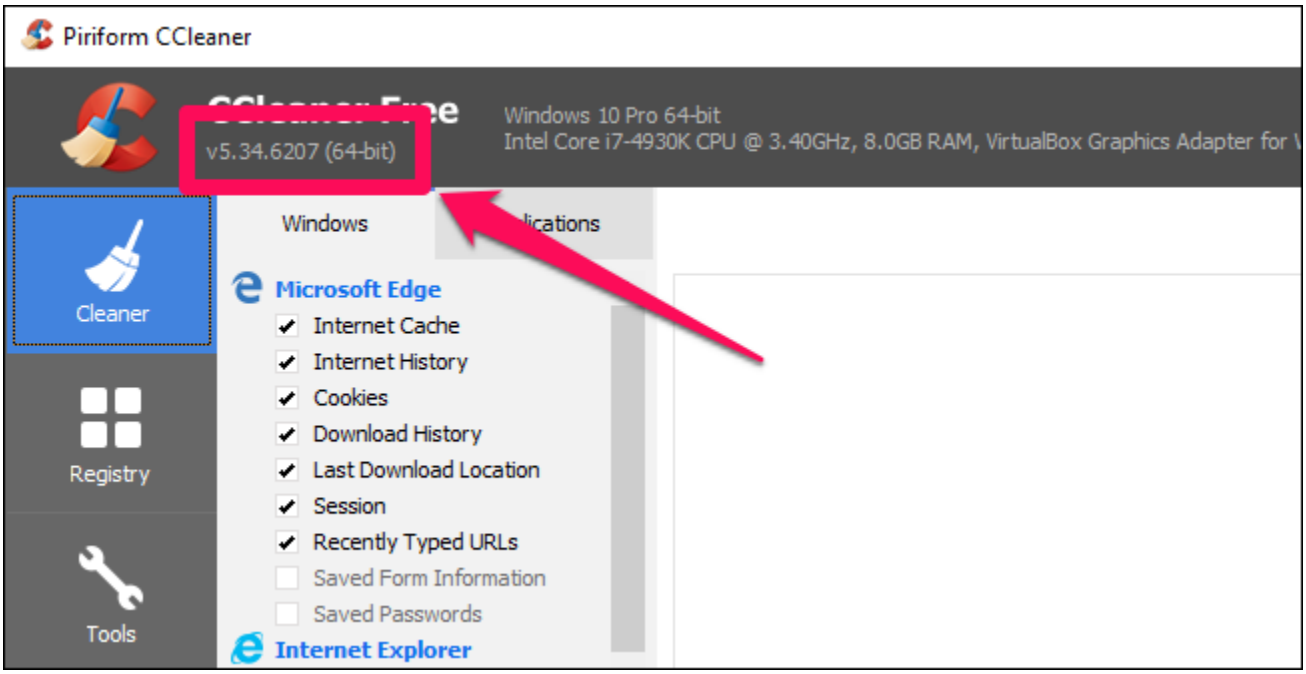
- Users running the 32-bit version of the application (not the 64-bit version)

- Users running version 5.33.6162 of CCleaner or CCleaner Cloud 1.07.3191, released on August 15th, 2017

Since many users likely use the 64-bit version of the application, and CCleaner Free does not automatically update, this is good news for a lot of people.

(*Update*: A few days after this news broke, a second payload was discovered that affected 64-bit users—but it was a targeted attack against tech companies, so it's unlikely most home users were affected.)

If you are on a 32-bit version of Windows and think you might have downloaded CCleaner during the affected timeframe, here's how to check what version you have. Open CCleaner and look in the top-left corner of the window—you should see a version number under the program name.



If that version is before version 5.33.6162, then you are not affected, and you should manually download the latest version now. If that version is 5.34 or later, your current version isn't affected, but if you updated CCleaner in between August 15th and September 12th, and are on a 32-bit system, you may still have been affected. (If you're comfortable going into the registry, you can open Registry Editor and navigate to HKLM\SOFTWARE\Piriform and see if there is a key labeled Agomo:MUID . If that key exists, it means you had the infected software on your system at one point in time.)

What Should I Do?

While nothing immediately harmful was discovered, Cisco Talos recommends restoring your system to a state before August 15, 2017 from a backup if you were affected. You should probably run an antivirus and MalwareBytes scan on your system and your backups to ensure no malware is left installed.

****

<u>Submitted by Mike Gerkin through Alyson Stroup</u>:

The following is the information regarding Century Link service for our winter residents and was in the last issue of Tech Times. Just in case you deleted it and you need the phone numbers here it is again:

Contact your Centurylink team today

WELCOME BACK

CenturyLink™

CenturyLink Winter Visitors' Connected Community:

Your property has aligned with our CenturyLink Superstition Springs store to make it easier for you to place your orders. We have created an exclusive support team as part of your property amenities to cater to the needs of your community.

- **PRICE FOR LIFE**
- **FREE ACTIVATION**
- **NO COST RECOVERY FEE**
- **NO CONTRACT**

It's very important to contact us at the special number below so that we can provide you with the best experience. We're here to assist you with your short term stay!

Call us to order New Service Today: 480-641-1680
Or come see us at Superstition Springs Plaza
1229 S. Power Rd Ste 107 / Mesa, AZ
EMAIL/SUPERAF@CENTURYLINK.COM

CenturyLink™

****

Submitted by Peggy Bullock:

Ransomware hack targeting 2 million an hour

By Francis Navarro, Komando.com

Watch out! A new ransomware attack has been detected and it's spreading quickly around the world with a rate of 2 million attacks per hour. It's likely higher.

According to an analysis from Barracuda Networks, the massive attack is launching around 8,000 different versions of the virus script. This makes it very difficult to put a stop to the attack.

The attacks seem to have originated in Vietnam, but some are coming from a multitude of other countries including India, Colombia, Turkey, and Greece. As the attacks spread, computers in more countries will be part of the hack.

"What's remarkable about this one is just the sheer volume of it," said Barracuda's Eugene Weiss.

Right now, the attack is still spreading rapidly. If you look at the WannaCry ransomware attacks this year, its effects can be devastating. That's why we wanted to alert you of this attack as soon as we became aware it.

What to look out for

Initial reports indicate that the conduit for this ransomware attack appears to be an email. Be on the lookout for any email with a subject of "Herbalife" or a "copier" file.

There could also be variants of the email subjects as the attacks spread so be on alert. One wrong click of a link in the email and all your files are overtaken by ransomware.

However, since this attack is still evolving as we speak, please look out for phishing and suspicious emails in general.

You need to know this too: Scammers are starting to take advantage of the huge Equifax breach. Click here to know what to look out for so you're not their next victim.

To continue reading the compete article, click on this link:

Ransomware Hack Attacking 2 Million per Hour?

****

Submitted by Mike Smith:

Our alert member, Mike Smith, who helps with the website, came across this article in AARP. Definitely an eye catcher – BEWARE!!

Scam Alert

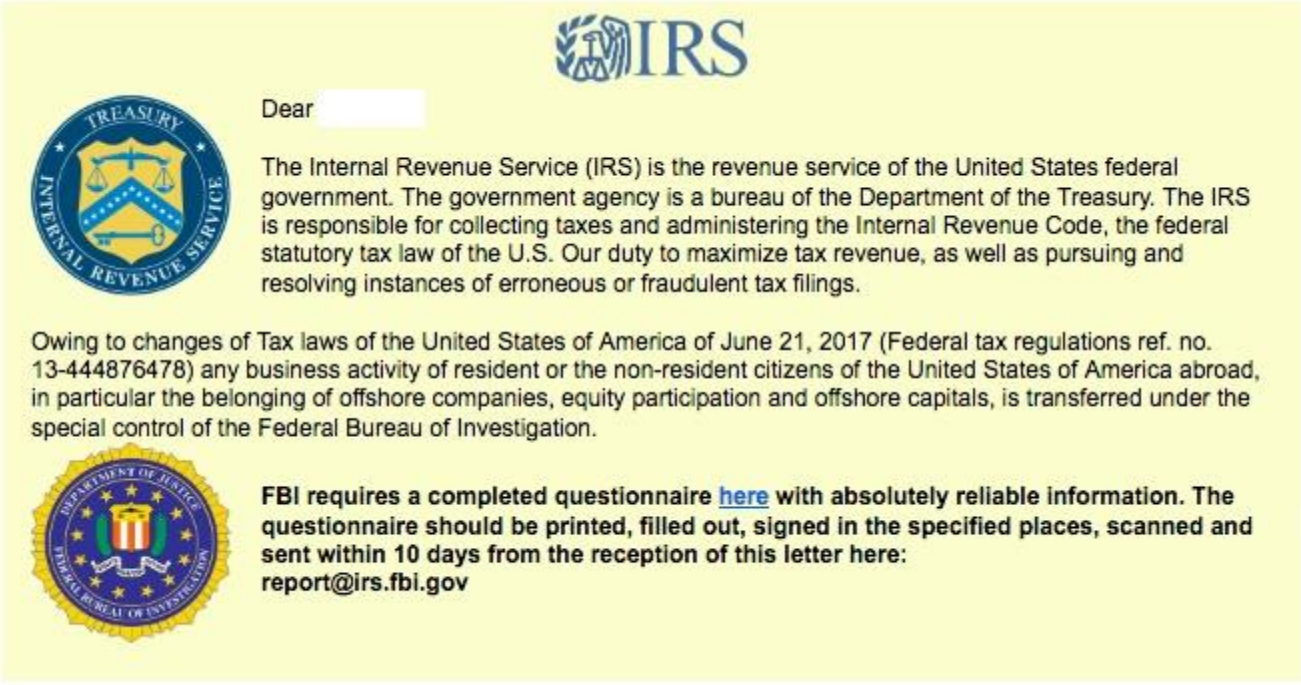
Posted on 09/08/2017

There's No Question About FBI 'Questionnaire' Email: It's a New Ransomware Scam

by Sid Kirchheimer |

The latest ransomware scam to seize control of computers and hold their contents hostage: an email with emblems of both the Internal Revenue Service and the Federal Bureau of Investigation that falsely demands completing an FBI questionnaire "required" by a new law on tax compliance.

It looks like this:



IRS

Dear

The Internal Revenue Service (IRS) is the revenue service of the United States federal government. The government agency is a bureau of the Department of the Treasury. The IRS is responsible for collecting taxes and administering the Internal Revenue Code, the federal statutory tax law of the U.S. Our duty to maximize tax revenue, as well as pursuing and resolving instances of erroneous or fraudulent tax filings.

Owing to changes of Tax laws of the United States of America of June 21, 2017 (Federal tax regulations ref. no. 13-444876478) any business activity of resident or the non-resident citizens of the United States of America abroad, in particular the belonging of offshore companies, equity participation and offshore capitals, is transferred under the special control of the Federal Bureau of Investigation.

FBI requires a completed questionnaire here with absolutely reliable information. The questionnaire should be printed, filled out, signed in the specified places, scanned and sent within 10 days from the reception of this letter here: report@irs.fbi.gov

While it may appear official, it's all a lie – an attempt to lure recipients to click on a link to access a questionnaire from the FBI (a longtime disguise by ransomware scammers), supposedly "required" because of a tax regulation that took effect June 21. But the cited regulation is bogus, and the link doesn't lead to a questionnaire; clicking on it downloads ransomware to prevent victims from accessing data stored on their device unless they pay money to scammers.

What's more, "people with a tax issue won't get their first contact from the IRS with a threatening email or phone call," IRS Commissioner John Koskinen notes in warning about this scam. Any official correspondence about personal tax or other issues from that or other federal agencies will come by U.S. mail – not by email, phone call, text message or social media posts.

Like recent ransomware attacks – notably WannaCry, which occurred last May and infected 230,000 computers in 150 countries, and Petya, primarily attacking computers in Ukraine in June – this new scheme is part of an ever-growing ransomware rampage. In addition to angling for ransom fees (usually requested in bitcoin) ranging from $300 to $600 per individual and tens of thousands of dollars from institutions, such attacks are estimated to cost over $5 billion this year in workplace-related loss of data and productivity.

After primarily threatening personal computers (including Macs) and institution-wide networks – including a record number of attacks last year – these scams are increasingly targeting smartphones, tablets and other mobile devices. During the first few months of 2017, mobile ransomware increased 250 percent, according to research by cyber security firm Kaspersky. And the U.S. is the world's favorite target for ransomware campaigns.

Your best defenses against ransomware?

1. Regularly back up important contents of your computer on an *external* hard drive or CD-ROM. This way, if you're hit with a ransomware attack, you can reinstall your files from that (it's worth repeating) *external* backup. You can set your computer to do this automatically – and once set, you can forget it … until you need those important files and photographs.

2. Click with caution. Don't trust links or attachments in emails from those you don't recognize, and carefully read body text in messages from those you recognize, looking for spelling and grammatical errors. Beware of those purporting to deliver, or seek, sensitive information not normally shared by email. While some ransomware-laden links purport to come from legitimate businesses, check the sender's address; scammers may use a Gmail.com, Hotmail.com or another free email service. If the message claims an impending delivery or other important news, go to that company's website by typing its address yourself, rather than depending on what's provided in emails.

3. Use reputable antivirus software and a firewall. **Keep software updated** and set to accept security patches, as they become available, to combat ransomware and other threats. You can also set your software to automatically run scans several times a week, if not daily.

4. Enable a pop-up blocker. Criminals regularly use pop-ups to spread malicious software. Preventing pop-ups is easier than making accidental clicks on or within them.

5. Avoid free online offers for screen savers and games unless you download them from trusted websites.

6. Don't pay the ransom. If you do because you didn't run regular backups, experts say there's no guarantee that scammers will provide the promised decryption key … and why would they risk exposing themselves? Payment might instead incentivize those or other cybercrooks to target your device for future attacks to keep the money coming. Instead, report any ransomware attempt or attack to www.IC3.gov and forward any IRS-themed scams to phishing@irs.gov.

****

From: Rick Heesen, Mike Gerkin, Mike Smith and Peggy Bullock