Southern Districts Computer Users Club Inc.

Supporting inexperienced users with local expertise

Vol.: — 20
No : — 02

February, 2020

SDCUCI NEWS

Contacts: Web Site: — http://sdcuci.com
E-mail: — sdcucinc@gmail.com

Newsletter Editor: David Porteous — daibhidhp@aussiebb.com.au

Meetings are held monthly on the third Wednesday at 7.30 pm, in the hall at the rear of St Mary's Catholic Church on the Corner of Bains and Main South Roads, Morphett Vale

Cost $3.00 per person per meeting. This includes a copy of our Newsletter, plus coffee/tea and supper

Visitors are most welcome

After 3 visits, you are requested to become members

Annual Subscription:
Single — $20.00
Family — $30.00

Both Novice and Experienced computer users will be most warmly welcomed

The Brownpaddock Chatter

Fearmongering scammers are using the coronavirus crisis to install dangerous malware onto computers.

Unsuspecting victims are sent an email warning coronavirus has been discovered in their local area, with a file attached regarding infection prevention measures.

Cyber security experts warn the attached file contains a dangerous type of malware campaign capable of stealing banking logins, financial data, and even emptying cryptocurrency wallets.

The **coronavirus** is being used by scammers looking to exploit unsuspecting victims. Known as Emotet, the trojan is attached under the guise of pdf, mp4 and docx files.

Users who open the attached file are infected with the malware, which can go undetected by antivirus software.

Increasing the likelihood of further infection, Emotet can also forward itself to every email contact of a victim. Forwarded emails that arrive in unsuspecting inboxes may appear innocent enough but may be anything but!

What to do if you receive one of these scam emails

If you receive emails from an unknown source, be very wary! - best to delete them immediately.

Never click on links or open attachments in an email unless you are sure of the sender. ! ! !

James Brownpaddock

A True Work-related Story by the Editor

As you probably know my other life was spent with the Adelaide City Council as their Chief Valuer and Property Manager. There are lots of stories from that period of my life. Here's one of them:

I had just been appointed as Chief Valuer following the retirement of my previous boss. My new duties included undertaking a rating valuation of the CBD. The Golden Rule belted into me by my now ex-boss was ALWAYS INSPECT THE PROPERTY. It was actually very good advice but, evidently not always followed by Himself!!

Some of you may vaguely remember the northern side of Rundle Mall at the King William Street end about 30 years ago. On the corner was Haighs Chocolates then a couple of other shops followed by a shoe shop and a lingerie shop. We'll stop there.

Walking along the Mall, I called on each shop in turn and, as I had been taught, had a look over each to determine the occupiable area on every floor.

It was my duty to advise each ratepayer of the valuation of their property subdivided into each separate occupancy. I sent the lingerie shop two notices — one for her occupation as owner/occupier of the lingerie shop and one for the shoe shop's occupation of her basement.

Later, I had a phone call from a very irate lingerie lady **stating categorically** that she did **not** have a basement. To cut a long story short, I met her on site and took her into the basement of the shoe shop. She was totally flabbergasted to see a large arch giving the shoe shop access into her basement which was full of shoe boxes. If only I had had a camera with me to capture her face! Why didn't my former boss pick that occupancy up — naughty, naughty!

Index

How to Scan E-email Attachments Online for Viruses

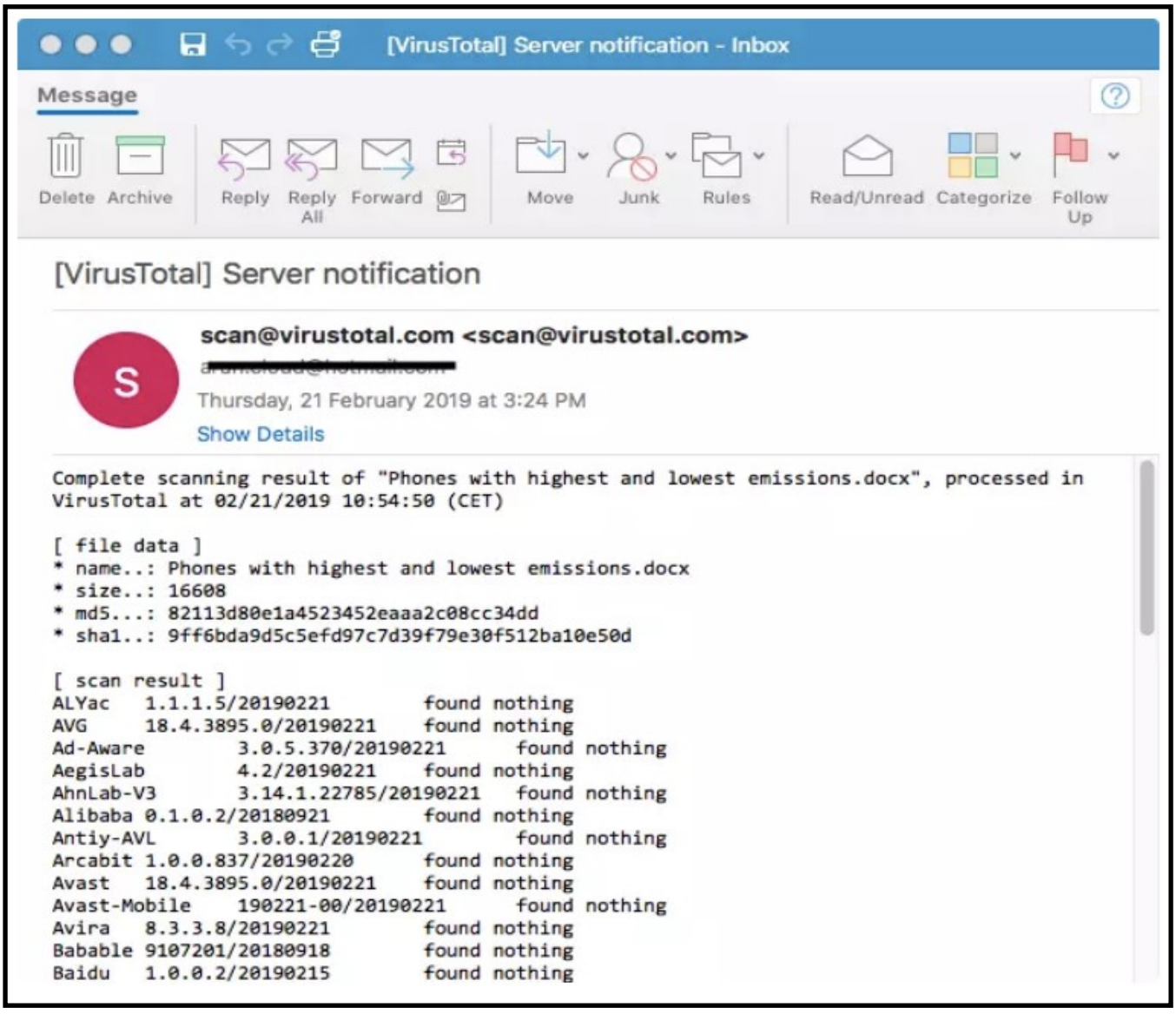
Most of us have antivirus software resident on our computers to protect our data files from malware. The Golden Rule is never to open attachments from unknown email addresses. But what if you want to get a second opinion about a suspicious email attachment? Can you scan the email attachment online for a virus? The answer probably is "no".

If you do need a second opinion, this is what you need to do.

Should you receive an email that sounds a bit fishy from someone, the first thing to do is contact Virus Total to allow them to sca n the attachment. Virus Total Online Virus Checking is an attempt from VT (Virus Total) for a better Internet.

To scan an email's attachment(s) using VirusTotal

Send an email with the suspicious file(s) as an attachment to Virus Total (see "Sending attachments to VirusTotal" on page 4). Virus Total will scan the attachment with many different anti-malware programs and send you the results the attachment generates from each (see below).



(continued on page 4)

(continued from page 3)

Sending attachments to VirusTotal

The following, is a step by step guide to scan an email attachment online for a virus.

1. **Right click** the attachment and select "Save to Desk top". A confirmation box should indicate that it has been saved to the Desk top. Click OK. Or **right click** on the item and select "**Save as"** then navigate to where you want to store the attachment and click "Save". Arguably, the former is the better choice of the two. UNDER NO CIRCUMSTANCES **LEFT CLICK** THE ATTACHMENT as that will open it which is the last thing you want to do until it has been verified as virus free.
2. Create a new email addressed to "*scan@virustotal.com"*;
3. If you want the Virus Total Online Scanner results in plain text, write "**SCAN**" in the Subject line; if you need an XML version as well, write "**SCAN+XML"** in the Subject line;
4. Attach the **Attachment** that you saved to the email you have just created addressed to "*scan@virustotal.com"*;
5. Hit the Send button.

You can also "Forward" the whole email together with the questionable attachment to "*scan@virustotal.com"* and write *SCAN* in the subject line. In this case there is no need to save anything.

As indicated on the previous page, the reply from Virus Total will show you the results in the format you asked for. It may take some time to reply if the load is high on their server. There is no need to resend the email.

You can see the details in the email from VirusTotal. If you selected SCAN+XML, you will get a plain text message and an XML coded page. If you opted for XML, it might take a bit longer to process and you may have to wait for a while. 

In the January issue of the SDCUCI NEWSLETTER I wrote a practical article about what to do now Windows 7 is abandoned by Microsoft.

Below is a rather different approach to the same subject — keeping yourself safe if you still want to keep using Windows 7. Read on! Ed.

How To Keep Using Windows 7 Safely After Support Ends

by Leo A. Notenboom

Yes, it'll be possible to keep using Windows 7 after it's no longer supported. However, doing so safely will depend on you.

I want to keep using Windows 7, but support is ending. Am I screwed?

No, you're not screwed.

You may very well be able to keep using Windows 7 safely, just as a small number of people continue to use Windows XP to this day. (*Including our Editor).*

You simply have to take responsibility for keeping yourself safe — even more than before.

Keeping Windows 7

The analogy I used in the previous version of this article for Windows XP was this: it's like keeping your old 1957 Chevy that still runs great.

Sure, it's a simpler vehicle; it has no seatbelts, air bags, navigation system, backing-up camera, anti-lock brakes, nor whatever else we take for granted on modern vehicles. Getting leaded gas or an equivalent is a bit of a problem, and driving the old girl requires a different skill set — for example, do you still remember how (and why) to pump the brakes?

And, of course, when something fails, you have a problem. You won't easily find a repair shop to help, not to mention replacement parts, and there certainly won't be any fixes or recalls.

As long as you're willing to work around all that, you can certainly keep driving it until it fails beyond repair.

Staying safe with Windows 7

To be honest, there's nothing really new or special you need to do to continue to use Windows 7 beyond its support window which ended on January 14, 2020. You just need to pay more attention to the things you should be doing already.

Keep your security software up to date. Keep all your other applications up to date. Be even more sceptical when it comes to downloads and emails.

Keep doing all the things that allow us to use our computers and the internet safely — with a little more attention than before.

Diminishing support

Over time, more and more software vendors will stop supporting Windows 7.

If that includes your security software, you'll need to find a replacement right away. Microsoft Security Essentials — my general recommendation — will keep working for some time independent of the Windows 7 cut-off date, but

(continued on page 6)

(continued from page 5) Microsoft won't support it forever.

That's true for any security software you run. As long as it keeps supporting Windows 7, you can keep running it. The moment it doesn't, you need to find an alternative.

Pragmatically, that's true for any software you run: at some point, Windows 7 support will be dropped, and you'll need to either find an alternative, stop using that software, or upgrade to a supported version of Windows.

Outdated software as a security risk

The risk of using any unsupported software, but particularly an unsupported operating system, is this:

At some point, a vulnerability will be discovered *that will not be fixed:* Malware will exploit that vulnerability

You'll then be relying *only* on your security tools — and your own common sense — to protect you. Depending on who you talk to, this is either almost certain doom or a complete non-issue.

Naturally, I fall somewhere in between.

As we've seen with Windows XP, predictions of catastrophe failed to materialize. As I said, there are folks happily and safely running it today. But there are also those who, faced with critical tools, favourite applications, and even hardware dropping support for the OS, have chosen to upgrade.

The same will likely be true for Windows 7; continuing to use it will eventually become more irritating than it's worth.

Exactly how long it'll take for that to happen depends, of course, on you.

Most important of all is that you take the steps to stay safe and remain skeptical.

Microsoft Supports Office on Windows 7 till January 2023

If you have been using Microsoft Office on Windows 7, you must know how long your version of Office and its products will be supported on Windows 7. The End Of Support for Windows 7 is on January 15, 2020. Whilst most of the software developers will gradually stop rolling out updates and fixes, Microsoft Office users seem to be in luck.

Microsoft Office will be supported on Windows 7 till January 2023

Windows 7 users should be happy because of the advantages coming from the Extended Security Updates subscription. Even if you do not pay, you will keep receiving malware signature updates for Microsoft Security Essentials. The same applies to Office products.

Microsoft Office 365 & Other Office Products

Office 365 users will keep getting security updates and fixes for the next three years, i.e., until January 2023. The company wants to help users to make the

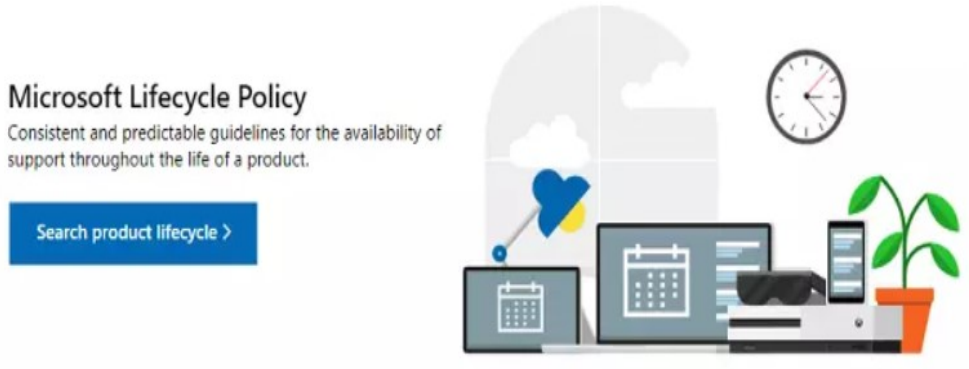
(continued on page 7)

(continued from page 6)

transition to Windows 10 or any other OS. However, the software will not receive any new features updates.

The rest of the products will get support until the end of their life cycle.

- Office 2010: 13/10/2020
- Office 2013: 14/04/2015 (Extended Support End Date)
- Office 2016: 13/10/2020



- Office 2019: 10/10/2023

While they also have Extended Support End Date, which spans till 2025, by that time, Microsoft will end the paid subscription support for Windows 7.

If your product is not listed here, please check the official page *(https://support.microsoft.com/en-gb/hub/4095338/microsoft-lifecycle-policy)*. There you can search for your product and check the end of life year.

You may face an issue because the OS is not secure, (i.e., the problem is a result of the combination of Office and an unsupported operating system.) Microsoft will offer no support. It is the primary reason most of the Office software will not receive any new feature update, but only bug fixes and security patches.

If you are planning to use Microsoft Office on Windows 7, make sure you secure the Windows 7 operating system (see pages 5-7 of the January edition of the SDCUCI NEWS and pages 5-6 of this issue for information regarding what you might consider doing.

The bottom line is "Use your common sense" 

Five Major Cybersecurity Trends for 2020

That well-known security firm, ZoneAlarm has this to say about Cybersecurity: 2020 is said to be a year that will bring on many changes in many different realms, but what does that mean for cybersecurity? With the rapid advancements in technology come better, more sophisticated tactics for cybercrime, and in return, pressing demand for innovative cybersecurity solutions.

(continued on page 8)

(continued from page 7)

Cybercriminals are more sophisticated at finding and exploiting vulnerabilities. The cost to the global economy was around $45 billion in 2018, and likely much more in 2019. Hence, spending on cybersecurity solutions will likely exceed $1 trillion between 2017 and 2021. So how can we protect ourselves?

1. Artificial Intelligence (AI) will be highly implemented

The increase of reliance on AI in cybersecurity allows companies to become more bulletproof against cyberattacks than ever before. Machine-learning technologies will be highly used, they will recognize weaknesses and prevent attacks in ways never used before.

On the other side of the coin, cybercriminals will also use AI to come up with more sophisticated and dangerous types of attacks. Look out for instances of highly intelligent impersonation of users, as their email and social media communication style will be highly sophisticatedly and accurately replicated to increase credibility.

Using AI, attacks will occur faster and on a much larger scale. Moreover, they will be nearly impossible to detect by traditional cyber solutions. Thus, it is imperative to get advanced AI-powered cybersecurity solutions**.**

2. Ransomware will keep on shining

Ransomware is every person's and organization's cyber nightmare. It is expected to stick around throughout the next decade. With a large pool of codes available, low barriers to entry, fairly easy execution, and high returns on investment, ransomware attacks are not going anywhere. In 2019, the number of ransomware attacks doubled and the number of new ransomware groups increased by 25%. This goes to prove that the demand for this type of cybercrime is not just high, but growing exponentially. Ransomware affected four US cities as recently as December 2019, alone, costing them millions in damages. So how do you protect yourself? Install strong anti-ransomware software such as ZoneAlarm Anti-Ransomware from *https://www.zonealarm.com/anti-ransomware*, which recently won PCMag's Editors' Choice for 2019 or BitDefender Total Security from *https://www.bitdefender.com.au/solutions/total-security.html.* There are others, but those are two of the leaders in the field.

3. Higher targeting of a wider variety of electronic devices

Have you ever heard of a vacuum takeover? It is possible for hackers to hack just about any electronic device. But hackers are after something very specific, and it does not involve your baby or your dog.

Say it is your mum's birthday and you call your florist to order her a bouquet. When you read your credit card numbers to them, often followed by your name and address, guess what? Any technological device around with a mic gets it as well.

4. Everything will be in the cloud (including our heads)

More and more individuals and businesses are transferring their data to the

(continued on page 9)

(continued from page 8)

cloud in order to avoid reliance on hardware storage alone, have greater location accessibility options, and easily share files among employees. In 2020, we can expect these numbers to soar. This shift to the cloud is not as safe and sound as it is made out to be, however. The cloud is still relatively new technology, and if not properly protected, it can be more prone to hacking. A prominent cause of cloud breach is password protection. People tend to follow the **very bad practice** of using the same password for everything, and if it is easy to crack, like "password" or "abc12345, (see page 7 of the May 2019 issue of SDCUCI NEWS) the attacker not only has access to your Gmail account now, they have access to your entire life on the cloud. What also makes cloud hacking possible is a user (yes, that means **you**) accidentally or mistakenly downloading malicious files that seem innocent but, in reality, grant the hacker access to your device and accounts.

Although saving your files to the cloud makes life a whole lot easier, it opens its doors to a number of cyber threats of a much higher magnitude than ever before, as hackers gain access to practically everything in one central location. For example, this past November, 1.2 billion (yes that's right BILLION) records were found exposed on a single cloud server. For these reasons, it is crucial to use secure cloud services, strong passwords, and install phishing protection on your devices. A good one to try is "ZoneAlarm Web Secure Free", a Chrome extension that protects your devices from entering and inserting your credentials into phishing sites and downloading malicious files. There are others—some free and some you pay for but not always better.

5. The 5G network threats will be increased

5G technologies are set to commence this year and are expected to dramatically change the tech game. It is all about "SPEED". Everything – and I mean everything – will become much faster. Unfortunately, with this great change comes a great opportunity for hackers. It isn't the security of the 5G networks that will cause all the havoc, on the contrary, 5G technology has better verification of users and stronger encryption of data than ever before. Integrating the Internet of Things (IoT) devices not yet equipped to handle advanced attacks (and are harder to update like smartphones and computers) leaves vulnerabilities wide and open. New technologies are a better target for hackers than well-established ones as they tend to pose greater vulnerabilities, and 5G is no different.

Conclusion:

Without a doubt, 2020 will be the year for considerable changes in tech. As you enjoy the fruit of these cutting-edge technologies, never **assume** you are protected. Apply best practices to your online security, like selecting two-factor authentication and using hard-to-crack passwords. Using the best and most comprehensive security software you can find for your PC and mobile is essential to protect you against zero-day attacks with advanced features, such as zero-phishing, anti-ransomware, threat extraction, and more, along with traditional yet powerful security features such as antivirus and firewall.

Our President has asked that I include a rather different article about the end of Support for Windows 7. Naturally, his wish is my command, so have a look at page 5 for a different take on this subject.

On page 6 there is information about a reprieve for Windows 7 users of the various iterations of Microsoft Office. This particularly relates to security updates. Depending on your version, Office 365 security updates will continue until 2023. However, there will be no feature updates.

Take the time to have a **really good look** at your existing security. Is yours up -to-date? Does it cover ransomware? Carefully examine your passwords; test them out at *https://password.kaspersky.com/* or "*https://lastpass.com/howsecure.php,* both reputable organisations", but be very careful of others. Double check that you use a **very different password** for each situation that a password is needed. Have a look at the SDCUCI NEWS for May last year to ensure you don't use passwords that can easily be cracked. Oh yes ! And don't forget to change all your passwords several times a year, just to be sure to be sure!

Jest a Minute

~ Tonight's Topic ~

TWITTER: INSTAGRAM / # HASHTAG

CAMERON RAWLINGS

— For Your Notes —

Our March Members' Meeting

Backing up Devices ***Lindsay Chuck***

We have visited this topic before but tonight's presentation will be all encompassing over desktop: laptop: - PC and Apple - with information on tablets, Smartphones and iPhones.

A must "see" on "how to" implement backup strategies

MEETING RULES

We are allowed to use the facilities at the Hall at the rear of St Mary's Catholic Church, on the corner of Bains and Main South Roads, Morphett Vale in return for a small fee plus respect for their property. We ask for your co-operation in respect to the above.

Whilst we have no control over what our members do away from our Club meetings, piracy of copyright material cannot be condoned at our meetings. Please respect copyright laws at all times.

IT & COMPUTERS

Shop 6, 76 Beach Road
Christies Beach 8186 2736
(Same block as Woolies on Beach Road)
Contact: Jamie or Ash
For all your computing needs
available locally

Need help with your computer?
Looking to purchase a new one?
Need additional peripherals?
Home site visits available !

Looking for excellent customer and after sales service?

New Computers
Repairs
Virus removal
New software & Upgrades

Peripheral units:
Wireless Keyboard Mouse
Sound Boards & Systems
External & Internal Hard Drives

Tell IT & Computers
you are from
S.D.C.U.C.I.

S.D.C.U.C.I can
recommend the
customer service
offered by
IT&Computers