NEWS CYBER SECURITY

Vol. 5 | Issue 8 September 2020

Page 2 | Page 3 | Page 4 | Challenge | Closing

Welcome to the TXDPS Cyber Security Newsletter!

We hope this newsletter finds you in good health, physically and emotionally, especially as the new school year kicks off. Remember, the start of a new school year brings out the scammers in full force, and with most schools starting virtually, cybercriminals will be looking to take advantage of your kiddos spending more time online. We recently sent an email with a few tips to keep your young learners safe. If you'd like us to send it again or have follow-up questions, please don't hesitate to reach out. The new format of school is challenging enough so lean on us to help you stay cyber aware. Hang in there, parents! You're doing great!

Now, let's talk about our virtual situation as DPS employees, specifically, **video conferencing.** As many of us who work from home have taken our meetings online, we, too, are targets for cybercriminals with this bigger online footprint. So..how do we stay safe?

If you will be attending a virtual conference, here are a few key steps suggested by our cyber awareness vendor, SANS:

- **Update the Software:** Make sure you are always using the latest version of the conferencing software. The more recent and updated your software, the more secure you will be.
- **Configure Audio / Video Settings**: Set your preferences to mute your microphone and turn off your video when joining a meeting and enable them only when you want. Consider placing a webcam cover over your computer's camera to ensure privacy when you're not actively broadcasting.
- **Double-Check What's Behind You**: If you want to enable your webcam, be aware of what's behind you. Ensure you do not have any personal or sensitive information visible behind you during a call.
- **Don't Share Your Invite:** The invite link is your personal ticket to enter the meeting. Even if a trusted co-worker needs the link, it's much better they ask the conference organizer for their own invite.
- **Do Not Record**: Do not take screenshots of or record the conference call without permission. You could accidentally share very sensitive information if those screenshots or recordings become public.
- **Sharing Your Screen:** If you will be sharing your computer screen at any point, be sure to first close all other applications and remove any sensitive files from your computer's desktop. Also disable any pop-up notifications to help ensure you don't accidentally share embarrassing information.

Cyber Risk Management

When you visualize the term "cyber security" in action, you probably picture cutting-edge technology used for network monitoring and incident response. You imagine flashing security alerts on a wall of screens and a team huddled around a computer as an analyst leans into the screen cranking out code to thwart a hacker's attempt. Maybe you think of vulnerability scans and penetration tests and firewalls. Or maybe you think of "cyber security" as having spam emails filtered and websites blocked to protect you and our agency from would-be scams. You wouldn't be wrong - our Cyber Ops team does some really cool stuff!

But there is also another side of cyber security - a proactive approach known as risk management. The primary function of risk management as a whole is to allow business leaders to determine the best course of action based on the probability of a given outcome and the possible detriments of that decision. As organizations have digitized, Cyber Risk Management has become a pillar of an effective risk management strategy.

Our Cyber Risk team focuses on security control implementation, documentation, and compliance to ensure cyber security is addressed BEFORE an incident occurs. We rely on a combination of strategies, technologies, frameworks and user education (that means you!) to protect our agency against cyber attacks.

Wait...what is a "security control?" Good question. A security control is a safeguard that helps us manage our cyber risk and protect our critical data assets from intrusions, security incidents, and data loss. An example of a security control is having your account lock you out after a certain number of failed login attempts. They are important to our security posture, they just aren't as flashy as those cool Cyber Ops tools and buzzwords you may be familiar with.

To that end, we wanted to create this space to focus on more specific controls that you may encounter when interacting with our Cyber team. Essentially, we want you to know *why* we ask you to do the things we ask you to do. We don't intend to be a roadblock to your project for the sake of merely slowing you down. We want to partner with you to make sure your project is complete in the most secure way possible, a mutual benefit to the agency.

Be on the look out for more specific information and examples of cyber security controls in future issues!

Emotet is back and at DPS

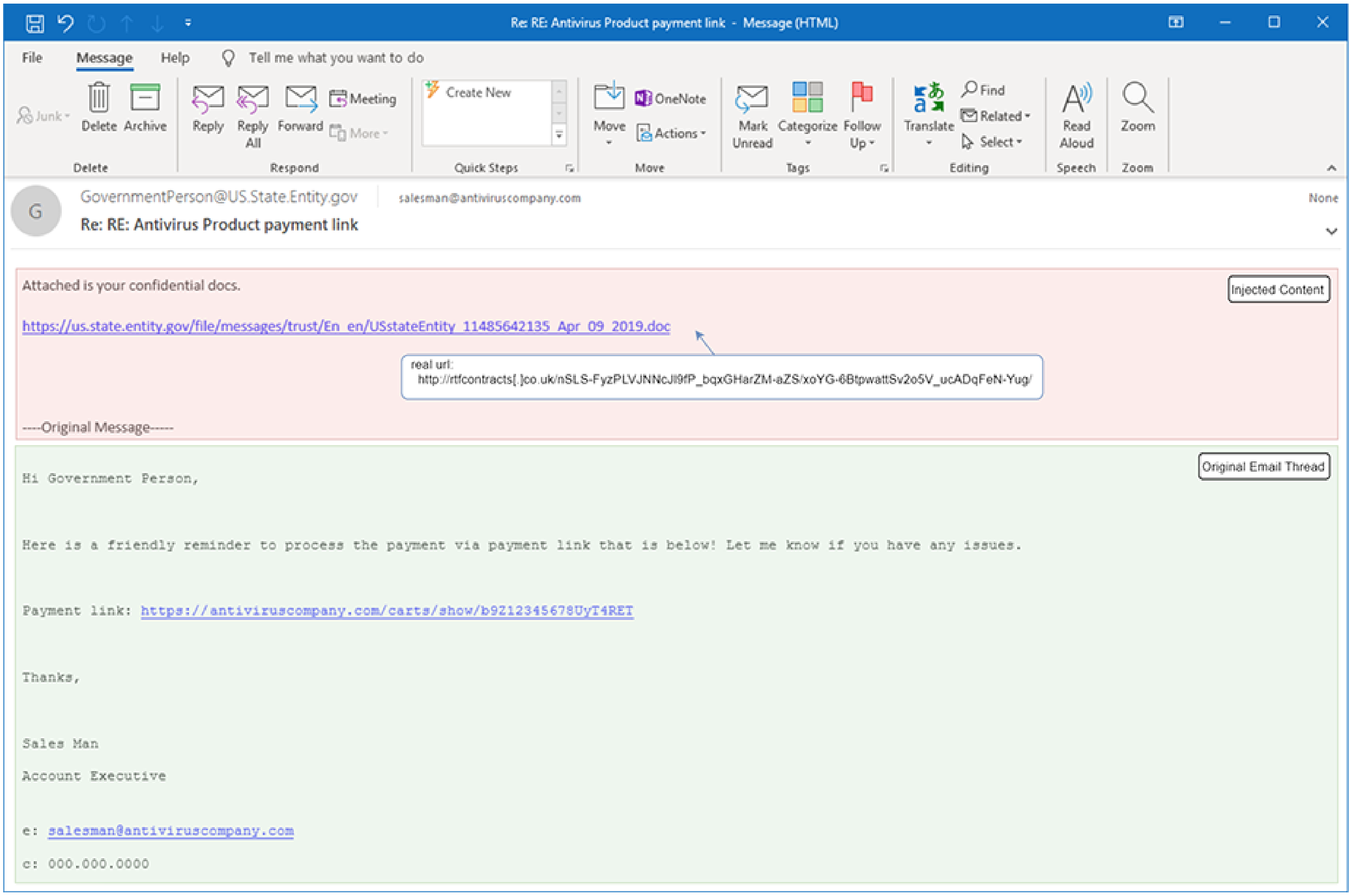
Thanks to our Cyber analysts, we've spotted a particular malicious threat here at DPS. After a 5-month hiatus, Emotet malware threat actors have resurfaced, sending well over 250,000 malicious emails. Some of which made their way here.

Emotet is a malware variant that continues to evolve over the years, quickly becoming more dangerous and is often combined with other types of malware such as information stealers, email harvesters, and ransomware. In less-nerdy words, it's big-time bad! And its favorite delivery method is phishing email.

What makes Emotet so effective is that it actually uses stolen, legitimate emails to create its phishing messages.

"Once they have swiped a victim's email, Emotet constructs new attack messages in reply to some of that victim's unread email messages, quoting the bodies of real messages in the threads," researchers explain. This means a phishing email will look very familiar to you…because it is. It's an actual email thread you've been a part of, only injected with malicious URLs and attachments with malware payloads.

Our DPS Cyber analysts have seen these reported by vigilant DPS users who didn't take the bait. So please continue to slow down when reading email and report anything that looks weird.



GovernmentPerson@US.State.Entity.gov salesman@antiviruscompany.com

Re: RE: Antivirus Product payment link

Attached is your confidential docs.

https://us.state.entity.gov/file/messages/trust/En_en/USstateEntity_11485642135_Apr_09_2019.doc

real url:
http://rtfcontracts[.]co.uk/nSLS-FyzPLVJNNcJl9fP_bqxGHarZM-aZS/xoYG-6BtpwattSv2o5V_ucADqFeN-Yug/

----Original Message-----

Hi Government Person,

Here is a friendly reminder to process the payment via payment link that is below! Let me know if you have any issues.

Payment link: https://antiviruscompany.com/carts/show/b9Z12345678UyT4RET

Thanks,

Sales Man

Account Executive

e: salesman@antiviruscompany.com

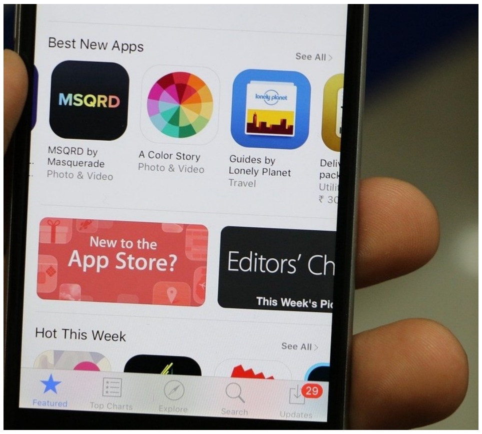
c: 000.000.0000

In the News

Report Claims a Popular iOS SDK is Stealing Click Revenue from Other Ad Networks

(By Catalin Cimpanu | August 25th, 2020)

In an explosive report published today, developer security firm Snyk claims it found malicious code inside a popular iOS SDK used by more than 1,200 iOS applications, all collectively downloaded more than 300 million times per month.



According to Snyk, this malicious code was hidden inside the iOS SDK of Mintegral, a Chinese-based advertising platform.

Snyk claims the iOS version of this SDK contains malicious features that sit silently in an iOS app's background and wait for a tap on any ad that's not its own. When an ad tap takes place, the Mintegratal SDK hijacks the click referral process, making it appear to the underlying iOS operating system that the user clicked on one of its ads, instead of a competitor's, effectively robbing revenue from other SDKs and advertising networks.

Logging user information as well

But while it appears that Mintegral is engaging in ad fraud, Snyk claims the SDK also contains other sneaky functions aimed at logging and collecting user-related information.

"Snyk further learned that the Mintegral SDK captures details of every URL-based request that is made from within the compromised application," the company said in a blog post today. This information is logged and then sent to a remote server, and includes details such as the URL that was requested and the device's IMEI number (a device's unique identifier).

Snyk did not release a list of iOS apps using the Mintegral SDK; however, the company said that the first version of the SDK where they found the malicious code was v5.5.1, released on July 17, 2019.

iOS users have no way of telling if they're using an app that secretly loads the Mintegral SDK, so there's little they can do to safeguard their private information and browsing habits. In an email today, Apple said it has spoken with Snyk researchers about their report, and that they have not seen any evidence the Mintegral SDK is harming users, at least for the time being.

As for Mintegral, the company vehemently denied the Snyk report, calling its findings as "false allegations."

Source: https://www.zdnet.com/article/report-claims-a-popular-ios-sdk-is-stealing-click-revenue-from-other-ad-networks/

A Few More Cyber News Stories:

TikTok's Security Boss Makes His Case. Carefully.
https://www.cyberscoop.com/tiktok-lawsuit-security-questions-roland-cloutier/

Hacking Humans - Many Times It is Less Sophisticated Than We Think (Podcast Episode)
https://www.thecyberwire.com/podcasts/hacking-humans/112/transcript

Russian Charged With Trying to Recruit Employee to Plant Ransomware in US Company
https://blog.knowbe4.com/russian-charged-with-trying-to-recruit-employee-to-plant-ransomware-in-us-company

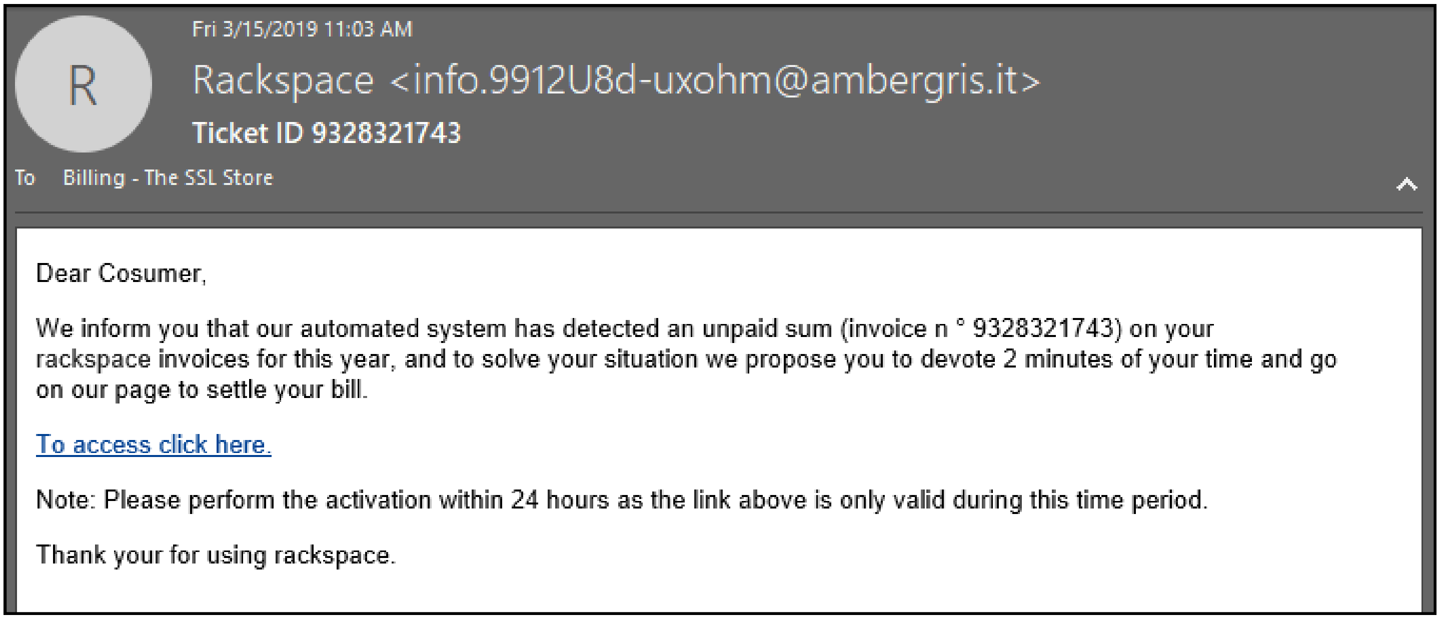
CYBER CHALLENGE

Find the Red Flags

This Month's Challenge

For this month's challenge, we'd like for you to find the red flags within these phishing emails. You can either use a drawing tool to highlight the areas in the email that should trigger a warning in your head about the validity of the email or just send your thoughts over to our Cyber Awareness group via email.

According to Verizon's latest Data Breach Investigations report, more than two-thirds of data breaches involve social engineering attacks such as phishing. So it's important you practice spotting the phish by identifying red flags, for both work and personal email. Don't get hooked!



Fri 3/15/2019 11:03 AM

Rackspace <info.9912U8d-uxohm@ambergris.it>

Ticket ID 9328321743

To Billing - The SSL Store

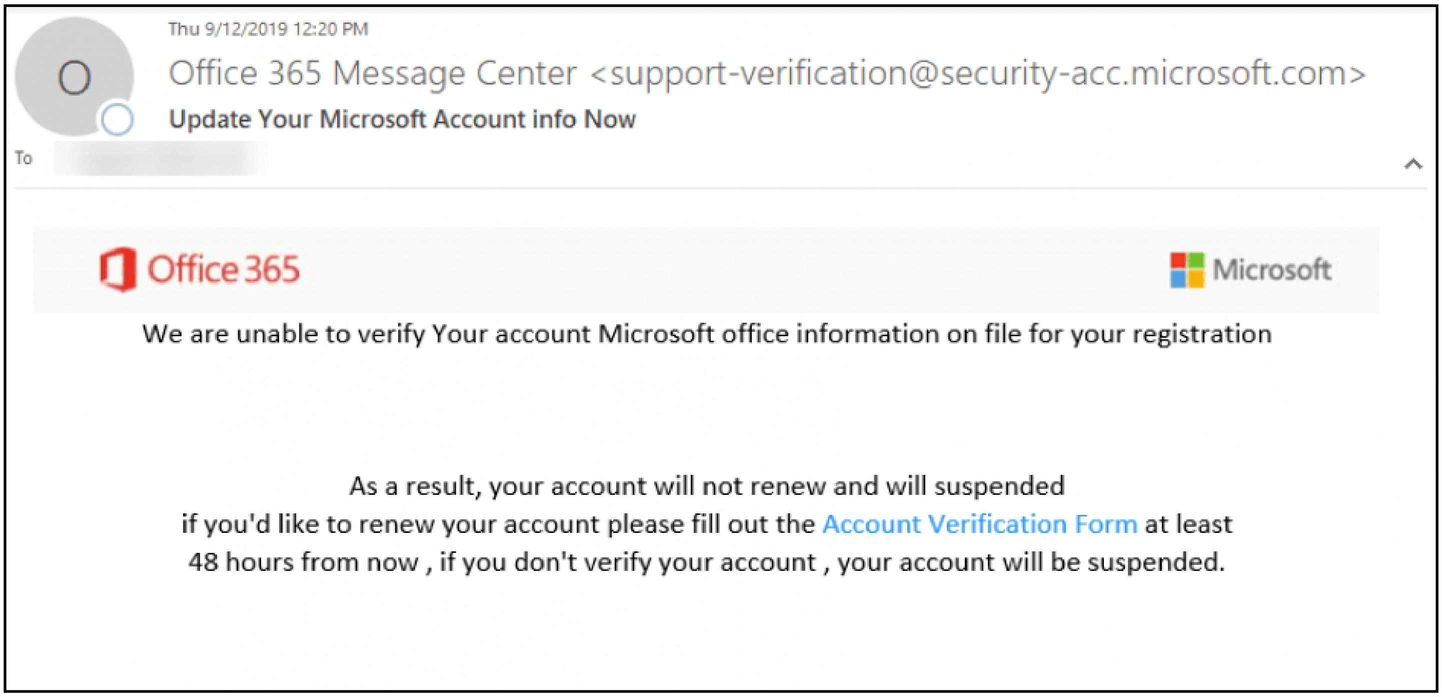
Dear Cosumer,

We inform you that our automated system has detected an unpaid sum (invoice n ° 9328321743) on your rackspace invoices for this year, and to solve your situation we propose you to devote 2 minutes of your time and go on our page to settle your bill.

To access click here.

Note: Please perform the activation within 24 hours as the link above is only valid during this time period.

Thank your for using rackspace.



Thu 9/12/2019 12:20 PM

Office 365 Message Center <support-verification@security-acc.microsoft.com>

Update Your Microsoft Account info Now

To [redacted]

We are unable to verify Your account Microsoft office information on file for your registration

As a result, your account will not renew and will suspended
if you'd like to renew your account please fill out the Account Verification Form at least
48 hours from now , if you don't verify your account , your account will be suspended.

</Closing Comments>

As we close this month's newsletter, we'd like to give a quick shout out to those of you who submitted your completed challenges from last month! We fully appreciate you taking a few minutes out of your day to engage with us!

A big THANK YOU to:

Faye Krueger
Lillie Petty
Debra Lewis
Erich Neumann
Rene Hess
Patti Cook

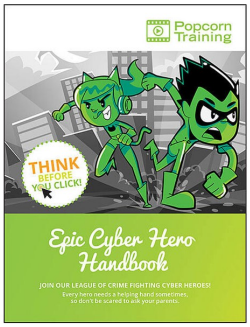
If we missed you, let us know!

Thank you for swinging by and checking out this month's newsletter! As your new Cyber Security Training Officer, I've enjoyed settling in and getting to know the DPS culture.

I'd like to leave you with this KnowBe4 Cyber Security Activity Kit for your young learners we mentioned at the beginning of this newsletter. Use this kit to help you talk to your kids about a few key cyber security concepts. Or feel free to color the coloring book and do the mazes yourself! https://www.knowbe4.com/cybersecurity-activity-kit

Activity Workbook 1

Activity Workbook 2



Captain Awareness Poster

I'm always open to feedback, either regarding this newsletter, our awareness training, or anything related to cyber security awareness here at DPS. If you have ideas to share, please send them my way (eric.posadas@dps.texas.gov). I've already heard from a few of you and have appreciated your thoughts. Keep them coming!

I look forward to continuing our partnership to bring cyber awareness to this agency and to our family and friends at home. And, as always, thank you for what you do for DPS and for your cyber vigilance!

- Eric Posadas

Share and Connect
Newsletter Archive Cyber SharePoint