AUREUSCONNECTIONS
THE TECHNOLOGY NEWS SOURCE FOR YOUR BUSINESS

QUARTERLY Newsletter

Special Issue!

Winter 2017 | Vol. 3, Issue 1 | www.AureusConsultants.com | Phone: (209) 230-5818

Inside This Issue...

DON'T GET "HOOKED" BY THIS NEW TAX SEASON PHISHING SCAM!

It's officially tax season and online scammers are already out in force! According to the U.S. Treasury, tax fraud cases have cost their victims over $50 million since 2013 – and this year it looks like these scams could be worse than ever.

Watch Out For Fake Emails.

This tax season, the IRS has issued an alert warning employers that a new business email compromise (BEC) scam is targeting payroll and HR departments. Through the use of various spoofing techniques, cybercrooks are sending fake emails which appear to be from your own organization, requesting a list of all employees and their W-2 forms. Once a scammer has this information they can file fraudulent tax returns, and even steal the identity of all your employees.

Don't Send Them Your Money.

In addition to asking for W-2 forms, scammers are sending another email often addressed to the comptroller requesting a wire transfer be made to a certain account. Companies who have fallen victim to both of these scams not only handed over W-2 information on all of their employees but also lost thousands of dollars in wire transfers. The IRS is urging all employers to warn their payroll and HR departments about these scams, and are even suggesting companies should create an internal policy to address the distribution of employee W-2 information.

What You Should Do:

If you or somebody in your business receives a W-2 scam email, you should forward it to phishing@irs.gov and place "W2 Scam" in the subject line.

If your business has fallen victim to any online scam, you should file a complaint with the Internet Crime Complaint Center (IC3), operated by the FBI.

Here are some phrases found in the fake emails, according to the IRS:

"Kindly send me the individual 2016 W2 (PDF) and earnings summary of all W2 of our company staff for a quick review."

"Can you send me the updated list of employees' with full details (Name, Social Security Number, Date of Birth, Home Address, Salary.)"

"I want you to send me the list of W2 copy of employees' wage and tax statement for 2016. I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me ASAP."

Top 3 Frauds Used By Crooks Online To Trick You

The internet makes it easier than ever to shop, pay bills, and even balance your checkbook from any device. While convenient, it's allowing criminals to reach into your private life further than ever before.

Phishing Email Scams

Cyber criminals send fake emails or messages on social media, which seem to come from an official source like a bank authority or social network representative. They try and persuade you to click on the link in their message which takes you to a fake access login page controlled by them. If you're not paying attention, you could give them your credentials!

Greeting Card Scams

These are e-cards that show up in your inbox and look like they came from a friend. If you click the link to download the card you download a virus instead. It may cause annoying pop-ups or even hold your data for ransom and your computer could start sending your private information to a server controlled by IT criminals.

Fake Antivirus Scam

One of the most common scams begins with a pop-up that tells you you're PC has been infected. The message itself contains a link to the virus, click it and you could end up with a Trojan or a "key-logger" virus on your system. Even worse, you could accidentally install Crypto-Locker - which is capable of blocking and encrypting your entire operating system.

DANGEROUS FACEBOOK SCAMS AND HOW TO AVOID THEM!

Some Facebook scams are harmless; they're more like hoaxes that just make you look silly. Unfortunately, some other scams can actually cause serious problems, install apps and programs that steal your information, or trick you into giving it up yourself.

FREE GIVEAWAYS

One of the easiest scams to fall for on Facebook is the free giveaway. They say you could win everything from gift cards to the new iPhone 7, you just need to fill out your information or take a survey. This way they trick you into giving them your personal information, or even downloading malicious software. Entering your cell phone number on a scam survey could result in bogus charges on your wireless bill. It's just better to avoid these surveys entirely.

VIRAL VIDEOS

You may be tempted to see the newest salacious celebrity video, but watch out for these fake posts. When you click to watch, you are told you need to update your video player first. If you click the update button, you will download and install a virus which will also share the scam automatically with your friends, so the virus spreads. As a firm rule, if you click any link on Facebook and it asks you to download something, always choose "No".

WHO VIEWED YOUR PROFILE?

This old gem has been around for almost as long as Facebook itself, despite the fact that FB has made it clear several times that there is no way for any app to show you who visits your profile. Any link or pop-up that says differently is either a prank or a scam, and the same is true for seeing who "unfriended" you.

CUSTOM PROFILES

This scam tries to con you into installing a fake Facebook app, so you can customize your profile. While there is no official way to change your layout, this app tricks you into giving the scammer your personal login information and a license to spam and scam your friends.

NIGERIAN SCAM

While this scam is most commonly found in fake emails sent to your inbox, it has also appeared on Facebook. However, Nigerian scammers on social media are pretending to be celebrities (like Prince Harry) and offering golden money-making opportunities that involve you sending them money first.

QUESTION:

If I happen to give them my credit or debit card as a result of the scam, *can I get my money back?*

Do you have a question for Ashley? *Email: asmithj@aureusconsultants.com*

ANSWER:

It depends. If you use a credit card, then most likely the funds will be reversed since it is the bank's or credit card company's money. However, when a debit card is used, it is *your* money and every bank has different policies when it comes to reversing funds due to fraudulent transactions. Either way, let them know immediately and cancel your card to get a new one.

"WARNING: YOUR COMPUTER HAS BEEN INFECTED WITH A VIRUS!"

WHATEVER YOU DO, DON'T CALL THAT NUMBER - IT'S A SCAM!

As you use your computer and browse the Web, you may occasionally run into infection warnings that appear to be legitimate but aren't. These anti-malware warning messages — appropriately called "scareware" — are designed to scare you into installing fake anti-malware programs that are actually malware in disguise.

HOW IT STARTS

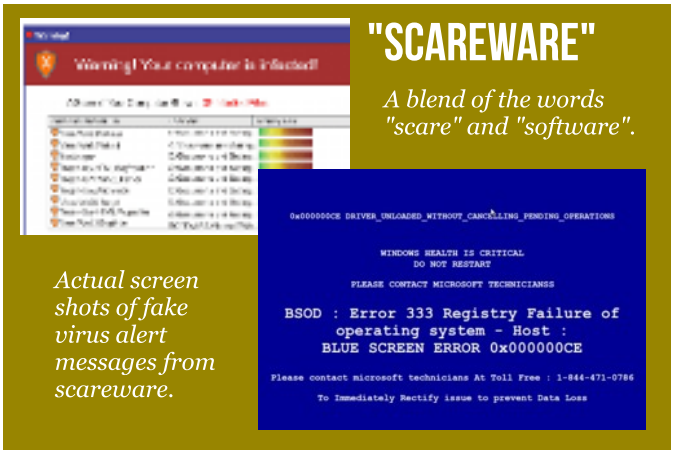
Usually, the first thing you'll see is a pop-up alert telling you a virus has been detected on your computer. There may even be several pop-ups that appear at once which can't be closed and are accompanied in some cases with loud beeps and a voice message. In every case, scareware is designed to trick you into calling a phone number where a "technician" will remotely takeover your computer to "fix" the problem. Whether or not they actually remove the virus, they will charge you a lot of money for their "services". Don't fall for it - it's a scam!

WHAT HAPPENS IF YOU CALL

Never call - most major companies like Microsoft and Norton don't make their support numbers easily available, since they need to regulate their call volume. If you do call however, the crooks will say anything to convince you that your computer is infected so that you'll download special software which allows them to control your computer remotely. Once they are in control, they will run fake scans that "prove" your computer has been infected with several viruses. This is when they will ask you for your payment information so they can "fix " the problem, costing about $40-$200 on average.

SIGNS THIS IS A SCAM

The first sign this is a scam is that you don't recognize the source of the alert. Any anti-virus product that you have installed would identify itself, and if you haven't installed one then you shouldn't be getting an alert. Another sign is that you are feeling pressured, trapped, and rushed to call a support number. A final sign this is a scam is that you don't actually know who you are calling and the person you speak to is vague and manipulative.



WHAT YOU SHOULD DO

If you don't call that number, you won't have anything to worry about. However, if you did happen to call and let that stranger into your computer, turn it off right away and terminate their remote connection. By this point they've definitely installed malicious software and you should take your computer to a local expert that you trust to fix it before you connect to the internet again.

If you authorized payment over the phone and gave these crooks your credit card or - even worse - your debit card information, you should call your bank or credit card company immediately and tell them you've been scammed. Don't beat yourself up about this, scareware tactics can fool anyone. The best thing you can do is learn more about how these scams trick people so you can avoid them in the future.

The Gold Standard Spotlight

At El Portal Dental Group, our mission is to help you achieve a sense of well-being by enhancing dental comfort, function, and appearance. We provide all services for your convenience such as teeth whitening, white fillings, root canals, ceramic crowns, veneers, bridges, dentures and implants, as well as clear and traditional orthodontics.

"We are a state of the art facility with a complex network of computers and we wanted a company that complemented our unique situation. We hired Aureus to help upgrade our network because they are prompt, courteous, and very professional. I would highly recommend Aureus' IT services to anyone – they are that good! "

"We have late and weekend hours. We accept most insurance and have flexible payment plans. If you don't have insurance, no worries, ask us about our Advantage Plan."

- Dr.Khang Nguyen, DDS

EL PORTAL DENTAL GROUP

3393 G STREET, SUITE B
MERCED, CA 95340
(209) 385-1479
WWW.ELPORTALDENTALGROUP.COM

- **Do you want a website, but you're afraid it's too expensive?**
- **Do you have a website, but it looks old and out-of-date?**
- **Do you wish you had more control over the content on your website?**

Visit: ***aureusconsultants.com/web-care*** and start designing your new website today!

TREND MICRO™

Worry-Free
Business Security Services

Advanced malware and ransomware protection from Trend detects and blocks ransomware encryption activities!

DON'T WAIT TO BE A VICTIM, CALL NOW FOR A FREE QUOTE: ***(209) 230-5818***

NEED FASTER INTERNET???

COMCAST BUSINESS

B4B

BUILT FOR BUSINESS™

If you have ever watched the clock while you were waiting for your browser to load, or been frustrated with buffering and slow internet speeds in your business, then now is the time to end your worries!

As a Comcast Business Authorized Connector:

- **We work hand-in-hand with Comcast to give you the best deal with the most discounts.**
- **We can offer you the fastest Internet connection in the Merced area.**
- **We'll handle everything so you'll never have to waste your time calling an 800 number again!**

If slow Internet connections are slowing down your business, call (209) 230-5818 or visit www.*AureusConsultants*.com to schedule your FREE consultation today!

Editor in Chief

Ashley Smith-Jenkins, President / IT Engineer
asmithj@aureusconsultants.com

Ashley has vast experience in the information technology field relating to computer and network services, including web development. For the past 21 years, Ashley has provided computer consulting and implementation for his customers. Ashley is a CompTIA A+ Certified technician and holds a Bachelor's degree in Business Administration from the California State University of Fresno.

Aureus Consultants, Inc. is a computer consulting firm and IT Service Provider headquartered in Merced, CA. We offer the gold standard in providing professional IT services with the most affordable options for local small businesses.

Contact:

AuREUS Consultants, Inc.
P.O. Box 3529
Merced, CA 95344-1529
Phone: (209) 230-5818
www.AureusConsultants.com