S.C.R.A.M. GAZETTE

# Tax Scams Afoot

**Tax Advisor Scams**

Social media manager at Experian, Michael Delgado, warned of this dire scam. Most consumers understand how precious their Social Security number is, but people using this scam attempt to get it from you anyway. Consumers should be on the look out for an email that asks tax professionals to update their IRS e-services portal information and Electronic Filing Identification Numbers, Delgado advised. The update links take you to a website that intends to capture your user name and password. This scam is so prevalent that the IRS lists a consumer warning on their IRS scam page.

It's important to guard your Social Security number and personal information. Don't fall victim to unverified attempts to steal this personal information. The IRS normally sends communication letters by U.S. mail, not email.

**Fake IRS Agent Scams**

The IRS is not going to call you and threaten you with arrest if you don't pay back taxes immediately with a credit card. Yet, according to Scott Goble, certified public accountant, financial planner and founder of Sound Accounting in Georgia, that is exactly how the fake IRS agent scam works. The fake IRS agent phones and informs you that you owe back taxes, and you must pay them immediately in attempt to scam your credit card number.

But the IRS doesn't operate that way. If you owe back taxes, the IRS will send you an official letter with a clearly stated reason for the letter. It will include ways to contact the IRS, how to resolve the matter and methods to dispute the allegations. If an IRS agent calls you demanding payment, just hang up on them — it's a scam.

## Cyberstalkers can peek through your webcam using one shockingly affordable software

You don't have to be a sophisticated cybercriminal to hack someone's webcam these days. New research unveiled simple software that allows almost anyone to peek into your personal space.

According to Komando.com sponsor Kaspersky Lab, new software called AdWind only costs a mere $70 per month and allows even those with basic computer skills to peep in on unsuspecting victims.

It all starts as a spear-phishing attack, in which victims are tricked into clicking on malicious links which will install malware on a computer without notice or any inclination.

That malware, for this particular instance, can grab photos, take video and record audio sound bites, which not only is creepy, but can be used in a number of shady ways like blackmail or extortion.

On top of that, the AdWind software can also snag passwords, monitor everything you do on your computer and transfer

files to steal your hard-earned money.

The software was first brought to light when it was used in an attack on a bank in Singapore. Since then, an estimated 443,000 people and businesses have been targeted around the entire world.

Even scarier is that the hackers using this software don't even need brains. According to David Emm, security researcher at Kaspersky, "The people using AdWind weren't cyberwarriors. They just had a low skill level, but were able to buy the code from people who developed it."

As always, if you're worried about becoming a victim, know that spear phishing is a more sophisticated version of phishing. It targets select groups of people that have something in common. They might work at the same company, for example.

In spear-phishing attacks, scammers will do research or steal information to send out legitimate-sounding emails. They might impersonate a person or organization from which you regularly receive emails.

Because spear-phishing emails often sound and look like the real thing, it's easy to become a victim.

Again, remember that most companies will never request personal information in an email. If you have any doubts, call the company to confirm. Just don't use any phone numbers provided in the email and don't reply or click on any links. Don't download any attachments or call any numbers in the message, either.

I recommend deleting suspicious messages right away. Never follow a link to a secure site like your bank or credit card company. Instead, manually type in the address into your browser if you need to get in touch.
Source: Mirror.uk

**NEXT SCRAM CLASS**
**March 9, 2016**
**At**
**11 a.m.**
**Niles Senior Center**

**Niles Police Department**
7000 W. Touhy Ave
Niles, IL 60714
847-588-6500
www.nilespd.com

**Connect with US!**

www.nilespd.com

## NEW MICROCHIP-ENABLED CREDIT CARDS MAY STILL BE VULNERABLE TO EXPLOITATION

By October 2015, many U.S. banks will have replaced hundreds of millions of traditional credit and debit cards, which rely on data stored on magnetic strips, with new payment cards containing a microchip known as an EMV chip. While EMV cards offer enhanced security, the FBI is warning law enforcement, merchants, and the general public that no one technology eliminates fraud and cybercriminals will continue to look for opportunities to steal payment information.

**What is an EMV credit card?**
The small gold chip found in many credit cards is most often referred to as an EMV chip. Cards containing this chip are known as EMV cards, as well as "chip-and-signature," "chip-and-pin," or "smart" cards. The name "EMV" refers to the three originators of chip-enabled cards: Europay, MasterCard, and Visa. EMV chips are now the global standard for credit card security.

**TECHNICAL DETAILS**
With traditional credit cards, the magnetic strip on the back of the card contains static personal information about the cardholder. This information is used to authenticate the card at the point of sale (PoS) terminal, before the purchase is authorized. When a consumer uses an EMV card at a chip PoS terminal, that transaction is protected using the technology in the microchip. Additionally, consumers will be able to continue to use the magnetic strip on the EMV card at retailers who have not yet implemented chip PoS terminals. When the card is equipped with a personal identification number (PIN), which is known only to the cardholder and the issuing financial institution, issuers will be able to verify the user's identity. Currently, not all EMV cards are issued to consumers with the PIN capability and not all merchant PoS terminals can accept PIN entry. EMV transactions at chip PoS terminals provide more security of consumers' personal data than magnetic strip PoS transactions. In addition, EMV card transactions transmit data between the merchant and the issuing bank with a special code that is unique to each individual transaction. This provides the cardholder greater security and makes the EMV card less vulnerable to criminal activity while the data is transmitted from the chip enabled PoS to the issuing bank.

**THREAT**
Although EMV cards provide greater security than traditional magnetic strip cards, an EMV chip does not stop lost and stolen cards from being used in stores, or for online or telephone purchases when the chip is not physically provided to the merchant, referred to as a card-not-present transaction. Additionally, the data on the magnetic strip of an EMV card can still be stolen if the merchant has not upgraded to an EMV terminal and it becomes infected with data-capturing malware. Consumers are urged to use the EMV feature of their new card wherever merchants accept it to limit the exposure of their sensitive payment data.

**DEFENSE**
Consumers should closely safeguard the security of their EMV cards and PINs. This includes being vigilant in handling, signing, and activating a card as soon as it arrives in the mail, reviewing statements for irregularities, and promptly reporting lost or stolen credit cards to the issuing bank. Consumers should also shield the keypad from bystanders when entering a PIN, as PINs are vulnerable to cybercriminals who work to steal these numbers to commit ATM and cash-back crimes.

The FBI encourages merchants to handle the EMV card and its data with the same security precautions they use for standard credit cards. Merchants handling sales over the telephone or via the Internet are encouraged to adopt additional security measures to ensure the authenticity of cards used for transactions. At a minimum, merchants should use secure servers and payment links for all Internet transactions with credit and debit cards, and information should be encrypted, if possible, to avert hackers from compromising card information provided by consumers. Credit card information taken over the telephone or through online means should be protected by the retailer to include encrypting digital information and securely disposing written credit card information.

If you believe you have been a victim of credit card fraud, reach out to your local law enforcement or FBI field office, and file a complaint with the Internet Crime Complaint Center (IC3) at www.IC3.gov.

# Southwest Airlines flight giveaway scams spread on Facebook

Once again Facebook users are being duped into liking and sharing pages, in the belief that they might be rewarded with first class flight tickets to a holiday destination.

Scammers have created Facebook pages that promise 400 free tickets to Las Vegas or 775 first class flights "for you and five friends to a dream destination of your choice anywhere in the world." And if that wasn't enough to trick you into doing the scammers bidding, they also trick you into thinking that you will be given $5000 in spending money too.

In the current example, the scams purport to

be official communications from Southwest Airlines, the world's largest low-cost airline, which has been the subject of many similar fraudulent campaigns on social networks in the past.

Here is a typical example of the current scam in action. It goes without saying that the offending pages are not run or sponsored by Southwest Airlines.

Rules for entry:
1. Share this photo and Comment "Thank You" below.
2. Like Our Page.
3. Click the "Sign Up" button on our page

In the case of this particular scam, which at the time of writing Facebook's security team has not deleted from the site, almost 23,000 users have shared the post with their online friends, and 14,500 have liked the page – all in the mistaken belief that it might help win them free airline tickets.