

Friday, June 15, 2018

In This Issue

- **URGENT: Reboot Your Router Now, If You Haven't Already**
- **Jackpotting: When Only Hackers Win the Prize**
- **How to Report a Phishing Attempt: Google, Apple, Facebook**

This Month's Tips:

Avoid downloading free software. Free software often contains viruses, adware, or spyware.

Only use trusted Wi-Fi networks when connecting to the Internet. Cybercriminals can create fake hotspots that provide free access points from which to steal your data.

Working remotely can carry some physical security risks. Use a laptop cable lock for long training sessions or conferences.

URGENT: Reboot Your Router Now, If You Haven't Already

Last month, the Federal Bureau of Investigation (FBI) issued a mandate for everyone to reboot their home or small business routers and network-attached storage devices. Cisco's threat intelligence division, Talos, estimates that the new malware threat, dubbed VPNFilter, has rapidly infected more than a half-million consumer devices across 54 countries.



Targeted devices include:

- Linksys routers
- MikroTik routers
- NETGEAR routers
- TP-Link networking equipment
- QNAP network-attached storage (NAS) devices

The Justice Department said last week that VPNFilter is the handiwork of "APT28," the security industry code name for a group of Russian state-sponsored hackers also known as "Fancy Bear" and the "Sofacy Group." The malware steals website credentials and can issue a self-destruct command, effectively rendering infected devices inoperable for most consumers. Rebooting your devices now will effectively disconnect you from the Sofacy network if you were infected with the malware.

To further disrupt the Sofacy network, the Justice Department sought and received permission to seize the web domain toknowall.com, which it said was a critical part of the malware's "command-and-control infrastructure." Now that the domain is under F.B.I. control, any attempts by the malware to reinfect a compromised router will be bounced to an F.B.I. server that can record the IP address of the effected device.

ACTION ITEMS:

- **Reboot your routers** and/or network-attached storage devices by unplugging and plugging back in the device.
- **Upgrade the device's firmware** (Google: your router name, updates. Be sure you select your router's official website.)

- **Select a new secure password** (Google: your router name, login. Follow the instructions to log into your router. If you have not logged in before, then you may be still using default credentials— admin/password. Be sure to change the username and password under the settings tab.)
- **Turn off all remote-management settings** (Once you are logged in, look for remote management settings under the Advanced Settings tab.)

Jackpotting: When Only Hackers Win the Prize

Jackpotting is an attack that allows an attacker to make ATMs spit out all of its cash. To do this kind of attack, criminals must have physical access to the ATM where they can use malware, physical hacking tools, or a combination of the two to make cash pour out of the ATM like the hacker won a jackpot (it's been recorded that 40 bills can shoot out of a machine in 23 seconds).



Up until this year, these attacks made their way through Asia, Europe, and Central America and had not yet been seen in the United States. Some of the reasons why it took as long as it did for jackpotting to reach the states are the level of security surrounding US ATMs and the extensive law enforcement capabilities.

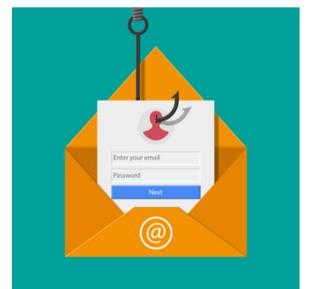
To reduce the risk of these kinds of attacks, banks have been advised to use end-to-end encryption, strong physical ATM locks, and two-factor authentication to access ATM access controls.

While these kinds of attacks do not directly impact individual bank customer's funds or personal information, someone could run the risk of finding an ATM without funds.

Should you spot someone loitering around an ATM, or watch piles of cash fall into someone's hands, make sure to report it to your bank.

How to Report a Phishing Attempt: Google, Apple, Facebook

Say you're scrolling through your inbox and receive an email from a major company, say Google, Facebook, or Apple, how do you go about letting them know someone might be sending phishing emails under their name? We've compiled a list of instructions for how to report phishing emails to various large and popular companies.



What is Phishing?

Phishing is a technique used by cybercriminals to acquire your personal information (such as credit card numbers or login credentials) by sending an email that is designed to look just like it came from a legitimate source

but is intended to trick you into clicking on a malicious link or downloading an attachment potentially laced with malware.

Report Phishing to Gmail:

While Gmail notes when you move an email to your Spam folder, they have also provided instructions on how to report these emails within Gmail itself:

1. On a computer, go to your Gmail account.
2. Open the message.
3. Next to Reply, click More. **Note:** If you're using classic Gmail, click the Down arrow.
4. Click **Report phishing**.

For further information on phishing attacks and emails, visit Google's support page here: <https://support.google.com/mail/answer/8253?hl=en>.

Report Phishing to Apple:

Apple recommends doing the following if you want to report a suspicious email:

- If you receive what you believe to be a phishing email that's designed to look like it's from Apple, please send it to reportphishing@apple.com.
- To report spam or other suspicious emails that you receive in your iCloud.com, me.com, or mac.com Inbox, please send them to abuse@icloud.com.
- To report spam or other suspicious messages that you receive through iMessage, tap Report Junk under the message.

For more information on Apple phishing emails, fake virus alerts, and other scams, visit Apple's office page: <https://support.apple.com/en-us/HT204759>.

Report Phishing to Facebook:

Facebook is aware of the multiple avenues scammers may take to steal your information or infect your devices. As such, they provide the following instructions and suggestions to protect yourself from falling victim:

Remember, Facebook will never ask you for your password in an email or send you a password as an attachment.

Scammers sometimes create fake emails that look like they're from Facebook. These emails often look like:

- Notifications about friend requests, messages, events, photos, and videos
- False claims that you went against Facebook's Community Standards
- Warnings that something will happen to your account if you don't update it or take a certain action
- Claims or offers that sound too good to be true (such as winning a Facebook Lottery)

Note: If an email or Facebook message looks strange, don't click on any links or open any attachments. Instead, report it to phish@fb.com or through the Report links that appear throughout Facebook.

Major organizations know that phishing emails aren't just bad for you, but also bad for them. As such, it is important to notify these companies when you spot a phishing email, so they can prevent it from being sent to someone else.

Inspired eLearning | 613 NW Loop 410 | Suite 530 | San Antonio, TX 78216

[Forward this email](#) to a friend.

© 2018 Inspired eLearning, LLC. All Rights Reserved.

All organizations with an active Security Awareness license are granted permission to republish any or all of the content in our Security Awareness Newsletter, as long as distribution of that content is limited to employees within the organization.