Monthly Cybersecurity Newsletter

April 2019
Issue

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson

Phishing is More Common and More Sophisticated

A recent Microsoft Security Intelligence Report (SIR) states that phishing attacks are by far the most frequent threat to cybersecurity. Not only are phishing attacks much more frequent, but they are also significantly more sophisticated. Cyber attackers can convincingly impersonate people and email domains, bait victims with fake links, prey on the emotions of people, and craft email attachments that look like what you may expect to receive. Cybersecurity leader, FireEye, recently stated that one out of 101 emails are malicious and email continues to be the ***#1 threat vector*** for cyber attacks. To make matters worse, FireEye detects an average of more than 14,000 malicious emails per customer per month that *get past security filters*. Other security researchers have found that one in every 99 emails is a phishing attack, and ***25 percent*** of those attacks bypass default security measures built into Office 365. In other words, Office 365's Exchange Online Protection (EOP) is clearing and delivering many phishing emails to its users.

Google researchers are also seeing more phishing attacks that are designed to thwart multi-factor authentication (MFA) protections. More organizations are embracing MFA as a means of stopping cybersecurity attacks that seek to compromise credentials. MFA incorporates an additional layer of authentication, rather than just a simple username and password. For example, an SMS-based verification code is sent to the end user's verified mobile phone. According to a Gmail security engineering lead, cybercriminals are incorporating mechanisms in their phishing schemes to capture and instantly use the combination of username, password, and a verification code. The attackers have adapted to SMS-based verification as part of the authentication process and have built detailed login pages that look like the original page to accept the additional information.

Phishing scams are becoming more sophisticated and more accessible to unsophisticated operators. The hacker trying to steal your information may not be a skilled cybercriminal. Hackers can purchase phishing kits, which clone popular websites and operate from temporary servers, from underground dealers for relatively small prices. These "out of the box" solutions simply require attackers to forward a prefab email with malicious links to their desired targets. Attackers also take advantage of current events to entice people who are interested or affected by a current situation. For example, see the article in the newsletter about the recent scams based on the Notre Dame Cathedral fire.

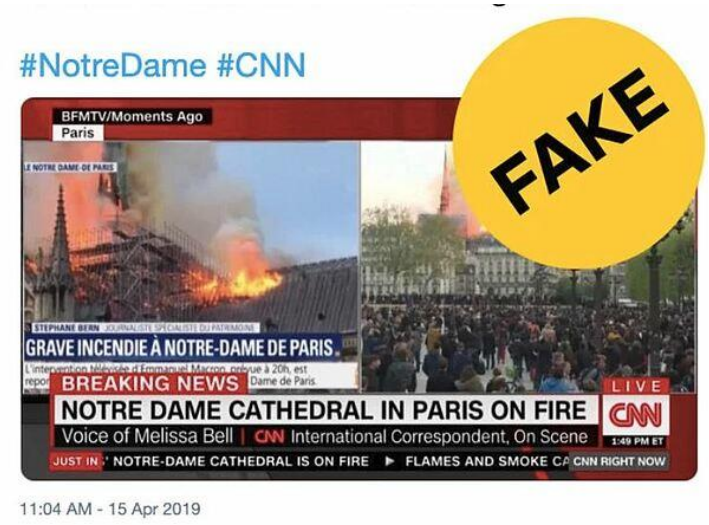
We should be thinking about cybersecurity as an onion. Technical controls such as spam filters, anti-virus (AV) and MFA are layers of the onion that can be used to help protect the core – our data. However, without ***end user awareness***, any technical control can be defeated. So, what can you do? Be cautious of email messages with the following characteristics:

"On the Internet, nobody knows you're a dog."

©The New Yorker Collection 1993 Peter Steiner
From cartoonbank.com. All rights reserved.

- Addressed to undisclosed-recipients.
- The From and the Reply-To addresses are different.
- Requests for personal or sensitive information.
- Promises of money or deals that are usually too good to be true.
- Threats or alarming messages.
- Random capitalizations, odd punctuations, misspellings, and improper grammar.
- Message is unexpected and/or out of character from the sender.
- Link in message will take you to a different address than the one that is displayed. Be sure to hover of link to see where it will go.

Be Aware of 'Fake News'!



#NotreDame #CNN

BFMTV/Moments Ago
Paris

LE NOTRE DAME-DE PARIS

STEPHANE BERN JOURNALISTE SPECIALISTE DU PATRIMOINE

GRAVE INCENDIE À NOTRE-DAME DE PARIS

L'intervention télévisée d'Emmanuel Macron, prévue à 20h, est repor Dame de Paris

BREAKING NEWS

NOTRE DAME CATHEDRAL IN PARIS ON FIRE

Voice of Melissa Bell | CNN International Correspondent, On Scene

LIVE CNN 1:49 PM ET

JUST IN ' NOTRE-DAME CATHEDRAL IS ON FIRE ▶ FLAMES AND SMOKE CA CNN RIGHT NOW

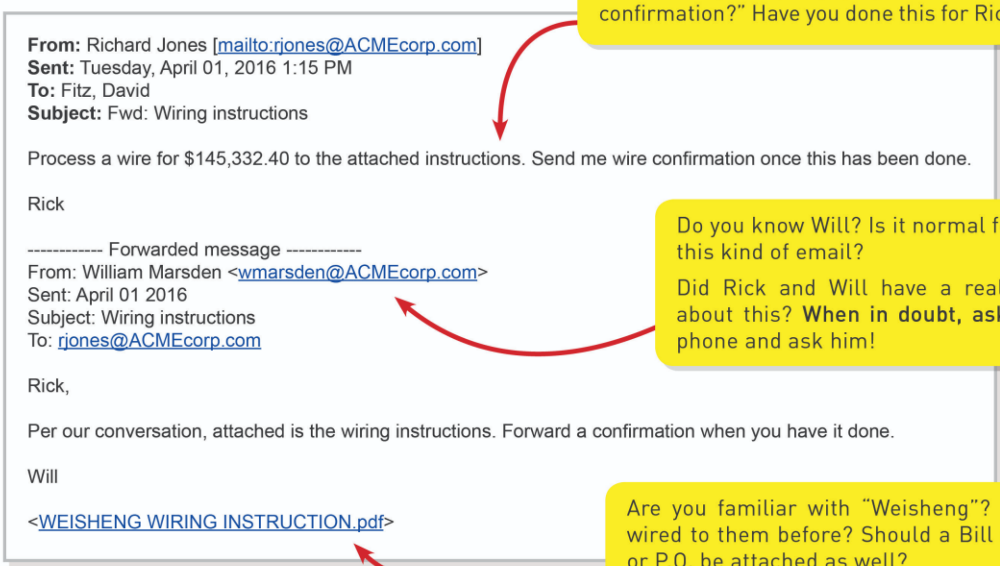
11:04 AM - 15 Apr 2019

Beware of scams that exploit current events. Cyber criminals waste no time to take advantage of what's going on in the world or what is popular in the news. For instance, the Notre Dame Cathedral in Paris caught fire this month and was barely saved from total destruction. Millions of people visit this iconic structure every year and many feel a powerful, and personal, sense of connection to it. Cyber criminals, however, were faster than ever to exploit the disaster into misinformation and social engineering. One Twitter account stated the fire was the work of terrorists, and another misrepresented itself as a major news organization and posted a fake quote from a congresswoman. Similar events of misinformation happened on YouTube and other social media outlets.

It is extremely easy to create malicious advertising campaigns that drive people to credential phish sites or simply infect their workstation with malware. Bad guys are exploiting the recent fire at the Notre Dame Cathedral in Paris. There are fake Facebook pages, tweets are going out with misinformation and fake charity websites are soon to follow. The bad guys are going to try to shock you and manipulate you into doing something in their interest. Do not fall for any scams, and do not click on any links in emails, texts or social media related to these scams. Whatever you see in the coming weeks about Notre Dame or any other current news event... **THINK BEFORE YOU CLICK**.

WHAT'S WRONG WITH THIS PICTURE?

If you receive a suspicious email, **use common sense** and ask yourself a few questions before clicking anything:



From: Richard Jones [mailto:rjones@ACMEcorp.com]
Sent: Tuesday, April 01, 2016 1:15 PM
To: Fitz, David
Subject: Fwd: Wiring instructions

Process a wire for $145,332.40 to the attached instructions. Send me wire confirmation once this has been done.

Rick

------------ Forwarded message ------------
From: William Marsden <wmarsden@ACMEcorp.com>
Sent: April 01 2016
Subject: Wiring instructions
To: rjones@ACMEcorp.com

Rick,

Per our conversation, attached is the wiring instructions. Forward a confirmation when you have it done.

Will

<WEISHENG WIRING INSTRUCTION.pdf>

What exactly are you paying for? What is a "wire confirmation?" Have you done this for Rick before?

Do you know Will? Is it normal for him to send this kind of email?

Did Rick and Will have a real conversation about this? **When in doubt, ask!** Pick up the phone and ask him!

Are you familiar with "Weisheng"? Have you wired to them before? Should a Bill of Lading or P.O. be attached as well?

Is the English correct, proper, and as you expect? *[Note that "Wiring Instruction" isn't plural. Chinese does not use plurals.]*

DID YOU KNOW?
PDF attachments are often infected with malware! You should only open them if they're sent from trusted colleagues.

Be on the lookout for emails that could be part of a targeted Spear Phishing campaign!

WHAT SHOULD YOU DO?

- ✔ Be suspicious of unknown emails and attachments.
- ✔ Do NOT respond, and do NOT open any attachments!
- ✔ Report all suspicious emails IMMEDIATELY.

© THE SECURITY AWARENESS COMPANY

KnowBe4
ON-DEMAND WEBINAR
10 Incredible Ways You Can Be Hacked Through Email
And How To Stop The Bad Guys

Email is still the *#1 attack vector* the bad guys use. A very high percentage of cyberattacks start with a phishing email, but email hacking is much more than phishing and launching malware.

Join Roger A. Grimes, KnowBe4's Data-Driven Defense Evangelist and security expert with over 30-years of experience, for this webinar where he will explore 10 ways hackers use social engineering to trick your users into revealing sensitive data or enabling malicious code to run.

Plus, he'll share a (pre-filmed) hacking demo by Kevin Mitnick, KnowBe4's Chief Hacking Officer where he captures an email hash with no clicks and no malicious code. To view this webinar, follow the following link: https://info.knowbe4.com/webinar-10-ways-hacked-email

Don't forget the following resources available to you. The following are some other **cybersecurity newsletters** the ESRMO recommends. We hope you find them beneficial and share them with your peers!

Security Awareness Newsletter: A monthly security awareness newsletter provided by KnowBe4 for all State employees. ***Note**: You must have a valid State employee O365 account.*

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2019

Security Tips Newsletter: A free monthly cybersecurity newsletter from the Center for Internet Security (CIS). The topic this month is ***Share Your Information With Care***.

- https://www.cisecurity.org/resources/newsletter

SANS OUCH! Newsletter: A free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***Making Passwords Simple.***

- https://www.sans.org/security-awareness-training/ouch-newsletter

The SANS Institute also provides *free* awareness **videos** and **webcasts**. The SANS Video of the Month may be accessed via the following link:

https://www.sans.org/security-awareness-training/video-month

The SANS Institute free webcasts may be accessed via the following link:

https://www.sans.org/webcasts/upcoming.

Cybersecurity Training and Awareness Plan

To combat the increasing security threats to the State's information systems and data, the Enterprise Security and Risk Management Office (ESRMO) will be providing, through the statewide Learning Management System (LMS), a series of cybersecurity awareness courses to be distributed every other month thoughout the 2019 calendar year. All Executive Branch employees and contractors are required to complete the assigned training modules by the end of each designated month. This training will be maintained in all employees' training records. The following is this year's Cyber Awareness Training Schedule:

Release Month	Lesson Topic	Lesson Title
March	Employee's Cyber Roles and Responsibility	Your role: Internet Security and You
May	Social Engineering	Phishing Fundamentals
July	Hardening Against Attacks	How to be a Human Firewall
**** JULY – ROLE-BASED TRAINING [DBA & APPDEV] ****		
September	Information Protection	Understanding and Protecting PII
October	*****OCTOBER - CYBER AWARENESS MONTH*****	
November	Insider Threat	Insider Threat

This year, the ESRMO will also add **role-based training** for those who are Application Developers or Database Administrators. Agencies are required to identify those individuals with significant security responsibilities who operate in those two positions. These individuals will be assigned an annual training module geared to their specific roles. The role-based training modules will be assigned by **July 1, 2019**, and must be completed within a 60-day period. The role-based training will be delivered through the training vendor portal, **KnowBe4**, from the following email address: ESRMO.Training@nc.gov. Contractors with state email accounts will receive an email with instructions on how to access their assigned training. Contractors are required to furnish the completion certificate to their supervisor for verification and retention.

KnowBe4
Human error. Conquered.

In addition to the scheduled training plan above, the ESRMO will also be conducting phishing exercises throughout the year via the preferred training vendor, **KnowBe4**. Phishing continues to be the *number 1 vector* used by malicious actors in order to gain access to systems and sensitive data. As part of our efforts to ensure employees do not fall victim to these attacks, the ESRMO will be conducting periodic unannounced phishing exercises on State government email accounts. Users who click on links in simulated phishing emails will be presented with additional training on ways to identify, detect and report these types of emails in the future. The goal of the phishing exercises, as well as the overall cybersecurity training program, is to raise awareness to users, decrease the possibility of compromise through phishing and other threats, and help better secure the North Carolina's data and assets. Remember…**Cybersecurity is Our Shared Responsibility.**

Have you considered **FedVTE**? The Department of Homeland Security (DHS) provides the FedVTE program, a free, on-demand, online cybersecurity training program with 24/7 accessibility. DHS offers FedVTE courses at **no cost** to government staff and contractors. With more than 60 courses, all cybersecurity professionals, aspiring and current, can build skills specific to their interests, work roles, and professional goals. Courses are added or updated regularly.

KEY FEATURES:

✓ Access **24/7**

✓ More than **60** available self-paced courses of varying proficiency – beginner to advanced

✓ Many popular certification courses including:

- Network +
- Security +
- Certified Information Systems Professional (CISSP)
- Windows Operating System Security
- Certified Ethical Hacker (CEH)

✓ All courses are aligned to the NICE Cybersecurity Workforce Framework.

✓ Individuals can take courses to build their knowledge, skills, and abilities in cybersecurity.

✓ Taught by experienced cybersecurity subject matter experts.

For more information and to visit FedVTE, please go to https://fedvte.usalearning.gov.

Do you have something to share? Is there a topic you would like to see in a future newsletter? The ESRMO encourages staff to share topics that will be of value to all agencies to foster better information sharing and awareness. If you have a suggestion for a topic that you would like for us to consider for a future newsletter, please send it to security@its.nc.gov.