Monthly Cybersecurity Newsletter

September 2019
Issue

NC DIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

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

Social Engineering Tactics!

We are all targets to cyber criminals who try their best to trick people into sharing confidential, personal information. Their most common way to attack us is via *social engineering*, which can occur through email, phone, face-to-face, or the internet. One security services provider states that 85% of organizations now experience some degree of phishing and social engineering attacks, which has increased 16% from just one year ago. The following are some of the kinds of social engineering attacks that are out there:

Phishing – Using e-mail to trick you into providing sensitive information, to include a reply to the original malicious e-mail, clicking on bogus links or opening attachments, and entering data.

Spear Phishing – Phishing attempts aimed at specific targets, such as HR or finance personnel.

Pretexting – A technique where a fake situation is created using publicly available details on the target where the information is used for manipulation or impersonation.

Scareware – As the name implies, a frightful pop-up attempting you to type in confidential, personal, and private information in order to fix an infected computer issue.

Vishing – Utilizing the telephone in attempt to trick you into providing valuable, most likely confidential, information.

Baiting – An attempt to hook you in by offering goods, such as a free device or gift card.

According to the Verizon 2018 Data Breach Investigations Report, phishing and pretexting represent 98% of social incidents, and 93% of breaches. However, e-mail continues to be the *most common vector of attack*. Countless phishing email messages are sent to unsuspecting targets every day. So, how can you guard against these attacks? There are several things you can look for that may be an indicator of a social engineering attempt.

- Look for mismatched URLs – hover your mouse over the URL and compare the address.
- Poor grammar and spelling could be an indicator that it is a phish.
- A request for personal information, such as SSN, user IDs, passwords, banking information, or a request for money.
- Correspondence that comes with a *sense of urgency*, such as your account may be disabled, or you may lose some funds.
- An offer that appears too good to be true.

- Unrealistic or unlikely threats.
- Content just doesn't look right.
- Open communication from a perceived authority, such as the Internal Revenue Service (IRS), or a financial institution.

Phishing emails also take advantage of current events and specific times of the year:

- Natural disasters or significant weather issues
- Global health scares, even flu season
- Financial or monetary concerns, like IRS scams
- Major political elections
- Holidays and celebrating events, such as international athletic events

For more information about social engineering, review the SANS article "Navigating the Phishy Social Engineering Ocean" by Cheryl Conley.

October will be National Cybersecurity Awareness Month (NCSAM), a collaborative effort between government and industry to ensure every American has resources they need to stay safer and more secure online. This year's NCSAM will emphasize personal accountability and stress the importance of taking proactive steps to enhance cybersecurity at home and in the workplace. The overarching message this year – Own IT. Secure IT. Protect IT. – will focus on key areas including citizen privacy, consumer devices, and ecommerce security.

Join the Multi-State Information Sharing and Analysis Center (MS-ISAC), Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), Cybersecurity and Infrastructure Security Agency (CISA) and National Cyber Security Alliance (NCSA) for a National Webinar on October 3 at 2 p.m. Learn how this year's theme "Own IT. Secure. IT. Protect IT." will encourage personal accountability and proactive behavior, and how you can get involved. For more information about NCSAM, visit the NCSAM 2019 page.

Also, be sure to check out the North Carolina Cyber Awareness Symposium that will be hosted by the N.C. Department of Information Technology (DIT) on Oct. 10-11. The Symposium will feature cyberbriefings from leading industry cyber partners, such as CrowdStrike, Tenable Nessus and Tanium. For more information about this event, visit the NC Cybersecurity Symposium page.

Are YOU the big phish?

Executives and personal assistants are prime targets for cybercriminals. **Don't become phish food...**

STOP.

It could be FAKE if:

F **Feeling:** it triggers an emotion
A **Action:** you are asked to action something
K **Know:** do you know the sender?
E **Expect:** were you expecting this?

THINK.

Hover over links and watch out for:

- **Numbers** https://192.45.36.72-bank.co.za/
- **Hyphens** "-" in-front of domain name https://secure-bank.co.za/
- **Strange name or country codes** https://BANK3.co.za

!

FBI:

$2.3 Billion Lost to CEO Email Scams

VERIFY.

Does it look like it is from someone you know?

Even if you know the sender, but the message seems slightly out of the ordinary, call to check.

Cybersecurity Newsletters

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

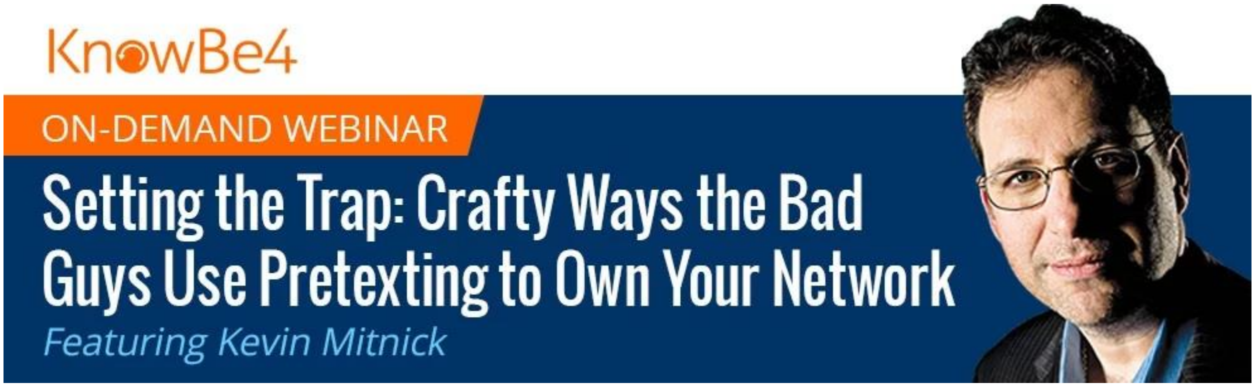
- ➢ https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2019

Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS). This month the newsletter covers ***Online Safety and Cybersecurity Tips for K-12 Kids, Family, and Friends!***

- ➢ https://www.cisecurity.org/resources/?type=newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***Scamming You Through Social Media?***

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


KnowBe4
ON-DEMAND WEBINAR
Setting the Trap: Crafty Ways the Bad Guys Use Pretexting to Own Your Network
Featuring Kevin Mitnick

Today's phishing attacks have evolved way beyond spray-and-pray emails that mass target victims. Instead, the bad guys have carefully researched your organization in order to set the perfect trap. And pretexting is the key.

Whether it's a phone call from an attacker impersonating your IT department or what seems like an innocuous email that ends up harvesting important credentials, the perfect pretext can lead to the bad guys owning your network before you know it.

In this webinar Kevin Mitnick, the World's Most Famous Hacker and KnowBe4's Chief Hacking Officer, and Perry Carpenter, KnowBe4's Chief Evangelist and Strategy Officer, show how the bad guys craft such cunning attacks. They dig into tactics for reconnaissance, target selection, creating a pretext, and launching an attack. And more importantly, they tell you what you need to know to protect your organization.

Kevin also shares new demonstration videos that will blow your mind! This is one webinar you will not want to miss! To watch this on-demand webinar, click here!

Triangle InfoSeCon is an annual Information Security conference and is the flagship event of the Raleigh Chapter of the Information System Security Association (ISSA). Their mission is to train and educate as many people as possible about the importance of Information Security. The chapter believes that Information Security is both the present and the future, and it is incumbent upon everyone to try to influence the decision makers of today and to train the security leaders of tomorrow.

The InfoSeCon event is a premier showcase of that mission and it provides information on a variety of cybersecurity topics and opportunities to network with over 1,600 cybersecurity professionals. This year's InfoSeCon will be on **October 25** at the Raleigh Convention Center. For more information and to register for this event, click here.

OWN. SECURE. PROTECT. IT.
2019
National Cybersecurity Awareness Month
#BeCyberSmart
The latest news and updates brought to you by
NATIONAL CYBERSECURITY ALLIANCE

Be A Cybersecurity Champion

National Cybersecurity Awareness Month (NCSAM) is almost here and the National Cybersecurity Awareness Month Champion program is a way to officially show your support for cybersecurity awareness. Champions represent those dedicated to making the connected world a safer place through awareness and education. Being a Champion is easy and does not require any financial support. NCSAM Champions include the following:

- Companies and organizations of all sizes
- Schools and school districts, colleges and universities
- Nonprofits
- Government organizations
- Individuals

Any individual or organization (state, local, private, etc.) can register to be an NCSAM Champion – it is easy and it is FREE! Organizations also have the opportunity to have their name listed on the NCSAM Champions website.

The National Cyber Security Alliance (NCSA) has provided more information and a webinar about this year's NCSAM theme and calls to action, how you and your organization can get involved and why you should register as a NCSAM 2019 Champion.

- **October** – National Cybersecurity Awareness Month (NCSAM)
- **October 3** – MS-ISAC NCSAM Webinar
- **October 10-11** – NC Cybersecurity Symposium
- **October 25** – Triangle InfoSeCon