LESSON GUIDE

# INTRO TO CYBERSECURITY

## Foundations and Threats

### 2.2.1 - Phishing

## Lesson Overview:

**Students will:**

- Define Phishing as the use of fake emails/websites to trick users into providing secrets.
- Emphasize that Phishing is one of the largest digital threats in the world and it is growing exponentially.
- Explain that phishing started with the "Advance Fee Scam" (aka Nigerian Prince letter).
- Identify key characteristics that help identify a phishing email.

**Guiding Question:** Why is Phishing considered the largest source of malware delivery and identity theft?

**Suggested Grade Levels:** 8 - 12

*This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).*

GALANTECH — with — GARDEN STATE CYBER

CYBER.ORG

THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

# Phishing

## Slide 1 - Intro Slide

## Slide 2 - Phishing

In recent years, Phishing has been the largest source of malware delivery and identify theft. In 2020 the Verizon Data Breach Investigations Report (DBIR) identified that credential theft, social attacks (i.e., phishing and business email compromise) and errors caused the majority of breaches (67% or more). In the DBIR report, Phishing was categorized as one of the top 4 cyber threats. AND PHISHING IS NOT EVEN MALWARE!! THERE IS NO REAL CODE OR PROGRAM!

## Slide 3 - What is Phishing?

In reading this definition and description of Phishing, it may seem like it falls in the category of "stupid user". But in fact, it can be very difficult to a spot a phishing email. In the next few slides, we will look at some examples and then try out a phishing test to see how well we can spot them.

## Slide 4 - Example of phishing

The Nigerian Prince letter is probably the earliest version of the phishing scam and definitely the most prolific. According to a Microsoft report, 51% of these "advance-fee" scam emails come from Nigeria. The basic story used in these emails is that there is a large sum of money held in a Nigerian bank account and the writer wants to transfer the money out BUT he needs a foreign bank account to deposit it to. He has chosen you because you are honorable and can be trusted, plus he will give you 20% or even 30% of the money just for helping him. All you have to do is provide your bank account # and your passport info so that we can make the transfer. Then everyone will be rich!! At least, the scammers will be!

Resource article: https://www.cnbc.com/2019/04/18/nigerian-prince-scams-still-rake-in-over-700000-dollars-a-year.html?&qsearchterm=nigerian%20prince

Optional video 9:39 minutes - use anytime during course when you need to fill some time:
Very funny Ted Talk video about replying to a Phishing Email:
https://www.ted.com/talks/james_veitch_this_is_what_happens_when_you_reply_to_spam_email

## Slide 5 - How to spot a phishing email

Here are some key tips to spotting a phishing email Video is 1:39 at YouTube: https://www.youtube.com/watch?v=5aJ0mZntZEc

Note, regular phishing makes a LOT of money. In August 2016, one of the largest phishers in the world was arrested (a Nigerian) and the police estimated that he had scammed over $60 million dollars. But to make the phishing campaigns even more effective and profitable, special phishing types have been developed. See next slide.

## Slide 6 - Special types of Phishing

- In **spear phishing**, research is done on a specific type of target - maybe all the people who live in wealthy, New York zip codes or all people who bank with Wells Fargo or all employees of Exxon. Based on the research, an email is created that is much more believable and is likely to get more victims.

- **Whaling** is taking the spear-phishing concept up another notch. This type of phishing targets only extremely wealthy or powerful individuals such as CEOs of major corporations.

- **Smishing** - becoming more common as the phone becomes the primary device for many people. The user is tricked into downloading malware onto their smart phone or device.

- **Vishing** - current examples are calls about car warranty or problems with your social security number.

Resource: https://www.cyber.nj.gov/informational-report/dont-take-the-bait-phishing-and-other-social-engineering-attacks

## Slide 7 - Phishing Attack or Spam Email?

We can easily be confused between Phishing and Spam because they both are unsolicited emails that have mal-intent like stealing your money or wasting your time. BUT there are key differences in characteristics detailed in this graphic. Most importantly, we should react to Phishing as if there is a potential attack and report it. With spam, it is enough to discard the email and mark the sender as spam.

## Slide 8 - ACTIVITY: Phishing IQ Tests

Time for the students to get some practice. On their devices have them access the Google Phishing Quiz website and each take the phishing quiz on their own. When completed they should review the answers to see what they missed.

Then have students go to the Cornell Phishbowl to see more current examples of phishing email. These were targeted at Cornell faculty and students - they are very convincing; it would be easy to fall for the scam! Students should select one email from the phishbowl that they might have fallen for. When everyone is ready, select 3 - 4 students to come up and show their selected phishbowl and describe why it might seem valid.

**Closure:** discuss whether this reso urce Cornell is providing is likely to be useful for user security awareness.

If time #1: Extra sites for Phishing tests:
https://www.opendns.com/phishing-quiz/
https://www.phishingbox.com/phishing-test

If time #2: Very funny Ted Talk video about replying to a Phishing Email
https://www.ted.com/talks/james_veitch_this_is_what_happens_when_you_reply_to_spam_email