PHIGHT THE PHISH
A PROGRAM TO BUILD CYBER HYGIENE AND SECURITY AWARENESS

PRESENTED BY
McAfee & Taft
WHO & WHY

- OKLAHOMA’S LARGEST LAW FIRM
- 70-YEAR HISTORY OF SERVING OKLAHOMANS IN LAW
- OKLAHOMA CITY, SPRINGFIELD (MO), TULSA
- CYBERSECURITY & PRIVACY
- LARGEST & MOST DIVERSE INDUSTRY GROUP
Social engineering attacks occur when an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems.
BUSINESS EMAIL COMPROMISE (or email account compromise) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests. **BEC is one of the most financially damaging online crimes.**
Phishing is a form of social engineering that uses email or malicious websites to solicit personal information or to get you to download malicious software by posing as a trustworthy entity.
TYPES OF PHISHING

SPEAR-PHISHING
WHALING
VISHING
SMISHING
SPEAR-PHISHING IS PHISHING TARGETED AT AN INDIVIDUAL BY INCLUDING KEY INFORMATION ABOUT THEM.
Whaling is phishing targeted at a high-profile individual to steal sensitive and high-value information.
VISHING IS PHISHING VIA VOICE COMMUNICATION TO ENTICE THE VICTIM TO ENGAGE IN CONVERSATION & BUILD TRUST.
SMISHING IS PHISHING VIA TEXT MESSAGES TO GET THE VICTIM TO CLICK ON A LINK, DOWNLOAD FILES AND APPLICATIONS, OR BEGIN A CONVERSATION.
Text Message
Today 12:22

【Apple】Dear [Name],
Your lost iPhone X 64GB Space Grey Has Been Found Today at 12:20 SAST.

View location: https://maps.icloud.com/0guk4

Sincerely,
Apple Support.
THE RISKS

OPERATIONS
REGULATORY INVESTIGATION & FINES
LITIGATION
DAMAGE TO REPUTATION
FINANCIAL DAMAGES
LOSS OF PUBLIC TRUST
9.6 DAYS
THE AVERAGE DOWNTIME FROM AN ATTACK
The financial risk

$125,697

Estimated ransom paid per event by municipalities
WHY ARE YOU AT RISK?

![Circle chart showing the proportion of risks in different categories.]

- Education: 25.0%
- Cities and Townships: 28.2%
- Counties: 13.9%
- Library: 4.3%
- Law Enforcement: 12.9%
- Other: 15.7%

THE ECONOMIC IMPACT OF CYBER ATTACKS ON MUNICIPALITIES
KNOWBE4, 2020
WHY ARE YOU AT RISK?

50 PERCENT

OF STATES DO NOT HAVE A COMMITTED CYBERSECURITY LINE-ITEM IN THE BUDGET
37 PERCENT OF STATES HAVE SEEN A REDUCTION OR NO CHANGE IN THE BUDGET FOR CYBERSECURITY OR TECHNOLOGY
ANATOMY OF A PHISH

SUSPICIOUS SENDER

GENERIC GREETINGS AND/OR SIGNATURE

CALL TO ACTION

SENSE OF URGENCY

SPOOFED HYPERLINKS

GRAMMAR & SPELLING

SUSPICIOUS ATTACHMENTS
ANATOMY OF A PHISH

From: Human Resources <HR@mcafeetaft.com>
Reply-to: Human Resources <HR@mcafeetaft.com>
Subject: RSVP for Company BBQ!

Sender email address is from your organization, but could be spoofed.

As a special treat this year for July 4th, we’re organizing a company barbeque. Your family members are invited too!

We will have games, live music, and a huge buffet for everyone to indulge in.

Find out how much food to buy.

Please [click here] to RSVP yes or no by the end of the day—and BE SURE to include how many guests you’ll have with you!!

Thanks!!

Human Resources

Sense of urgency. (Example: “Do this now!”)
ANATOMY OF A PHISH

Dear Member,

We recently detected unusual activity on your Apple ID.
To verify this ID belongs to you, check the link below,
sign in and then follow the instructions.

Verify now

Sense of urgency: "Example: "Do this now!"

Apple Support™

Sender email address is from your organization, but could be spoofed.

http://fleeckshop.be/modules/socialupgrade/dir/

Open
Add to Reading List
Copy
Cancel
[LEFT] BOOM [RIGHT]
WHAT KIND OF BOOM?

EVENT < INCIDENT < BREACH
LEFT OF BOOM: PREPARATION

WHEN IN DOUBT, REPORT IT OUT
MAKE PASSWORDS LONG & STRONG
MFA, IN EVERY WAY
HYPER-WARY OF HYPERLINKS
ALWAYS UP THE ANTI
TRAIN TO GAIN
Teach a person to see a phish, and they will stop phish for a lifetime.
THE BOOM: INCIDENT HANDLING

DETECTION & ANALYSIS
CONTAINMENT, ERADICATION & RECOVERY
POST-INCIDENT RECOVERY
Municipalities must focus on

People
Process
Technology
DOES OUR CITY HAVE AN INTERNAL OR EXTERNAL TECHNOLOGY TEAM?
DOES OUR CITY HAVE A DESIGNATED EMPLOYEE (FULL OR PART-TIME) FOR CYBERSECURITY?
DOES OUR CITY HAVE A DESIGNATED TEAM FOR CYBERSECURITY EVENTS?
DOES OUR CITY HAVE A PROCESS FOR ASSESSING CYBER RISKS?
DOES OUR CITY HAVE AN INCIDENT RESPONSE PLAN?
DOES OUR CITY HAVE A CYBERSECURITY TRAINING PROGRAM?
WHAT PLATFORM DOES OUR CITY USE FOR EMAIL AND OFFICE MANAGEMENT?
WHAT SECURITY TOOLS ARE ENABLED ON THIS PLATFORM?
DOES OUR CITY UTILIZE MULTI-FACTOR AUTHENTICATION FOR ALL OUR TECHNOLOGY SYSTEMS?
SASHA BELING
405-270-6011
SASHA.BELING@MCAFEE TAFT.COM

ZACH OUBRE
405-270-6023
ZACH.OUBRE@MCAFEE TAFT.COM

JOSHUA SNAVELY
405-270-6027
JOSHUA.SNAVELY@MCAFEE TAFT.COM

QUESTIONS?