Security Awareness Update

BOC Work Session

April 8, 2019

WAKE COUNTY
NORTH CAROLINA

Key Terms

- **Malware:** “hacking” software designed to disrupt, damage, or gain unauthorized access to a computer system.
- **Ransomware:** malware that encrypts files on a server or computer. The attacker then demands payment to unlock the files.
- **Phishing:** an email scam by which a user is duped into revealing passwords, personal or confidential information or unwittingly enabling illegal access to a network
- **Spear Phishing:** phishing focused on a specific individual, organization or business, often intended to steal data or install malware on a targeted computer.

Key Terms

- **Whaling Attacks:** a phishing attack that targets high-profile employees, such as the CEO or CFO, in order to steal sensitive information.
- **Advanced Persistent Threats (APTs):** an attack in which an unauthorized user gains access to a system or network and remains there for an extended period of time without being detected.
- **Social-Engineering:** an attack that relies on human interaction in order to manipulate users into breaking security procedures in order to gain access to systems, networks or physical locations.

City of Atlanta

March 23, 2018

Hackers Are Holding The City of Atlanta Hostage

August 6, 2018

Atlanta ransomware recovery cost now at $17 million, reports say

October 4, 2018

Why us? 6 months after ransomware attack Atlanta has no answers

Georgia Charges Iranians In Ransomware Attack On Atlanta

December 5, 2018 · 9:15 PM ET

Across the Country

October 12, 2018
Recovery Has Not Come Cheap for the Alaskan Borough Targeted by Hackers

November 21, 2018
City of Valdez, Alaska admits to paying off ransomware infection

January 14, 2019
Ransomware attack sends City of Del Rio back to the days of pen and paper

January 23, 2019
Sammamish declares emergency in response to ransomware attack

January 31, 2019
Spartanburg Co. library system refuses to pay ransomware

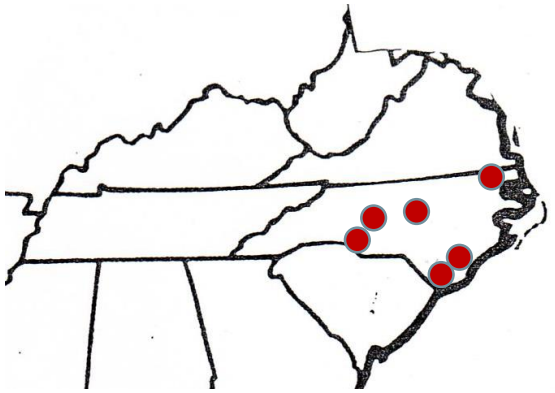
March 9, 2019
Jackson County paid online criminals $400,000 to stop cyber-attack, officials say

March 12, 2019
Ryuk Ransomware Attack Causes Delays at Boston Public Defenders' Office

March 25, 2019
Oregon Agency Reports Phishing Attack Affecting 350,000

April 2, 2019
City of Albany Latest Local Government Hit With Ransomware

In The Local News



October 15, 2018

Hackers hit Onslow County utility with ransomware attack

March 18, 2019

Orange County computer network hit by ransomware attack

October 16, 2018

In County Crippled by Hurricane, Water Utility Targeted in Ransomware Attack

March 19, 2019

Hackers demand ransom from Orange County for 3rd time in 6 years

December 21, 2018

Pasquotank-Camden EMS Hacking Incident Impacts 40,000 Patients

March 21, 2019

North Carolina County Suffers Repeat Ransomware Infections

- ~1.2 million citizens
- 10,000+ Connected Devices
- 3,800 Employees
- 17,000+ User Accounts
- 430TB Data Onsite
- Cloud Hosted Applications
- Regulatory Fines (HIPAA, PCI, CJIS, etc.)

It Only Takes 1

What Are We Doing To Protect the County?

People

Information Risk Management Core Team

Security Awareness Training

Phishing Simulations

Process

Policies & Procedures

Incident Detection and Response

Security Risk Assessments

Technology

Firewalls

Intrusion Detection Systems

Intrusion Prevention Systems

Internet Content Filtering

Email Security

Endpoint Protection

Multi-Factor Authentication

Vulnerability Management

Encryption

Security Awareness Program

Mandatory Training Modules (Quarterly)

PHISHME

Countywide Phishing Simulations (Quarterly)
Departmental Phishing Simulations (Random)

THE WIRE Get Connected. Stay Connected.

Security Articles

Security Awareness Program

>98%

Users that have completed mandatory security awareness training

Users reporting suspicious emails

Users susceptible to phishing simulations*

**5% lower than the baseline for governmental agencies.*