Wis Fresh Fruit & Vegetable Conference

Protect your business from Cyber Threats

Introduction

Mike Masino

Program Director

Cyber Security Program, Madison College

mmasino@madisoncollege.edu

Introduction

Denny Wright

Instructor Network Specialist Program, Madison College

dwright2@madisoncollege.edu

Co-Owner The Wright Way Farm

thewrights@thewrightwayfarm.com

Topics

- Phishing Attacks
- Weak Password/Authentication
- Malware
- Ransomware
- Social Media
- Web presence

Phishing Attacks

Phishing Attacks

Statistics:

- The most widespread threat
- Accounts for 90% of all breaches
- Over 12 billion in business losses last year

Phishing Attacks

What is it?

When an attacker pretends to be a trusted contact, and entices a user to click a malicious link, download a malicious file, or give them access to sensitive information, account details or credentials.

Phishing Attacks

Why is it difficult to defend against?

- Social Engineering is used to target unsuspecting people
- The attack comes down to a person making a decision
- The best defense is educating users

Phishing Attacks

What can you do?

The best defense against phishing style attacks is recurrent Security Awareness Training for staff and employees.

- Madison College
  - https://my.madisoncollege.edu/app/catalog/showCourse/MATC1/006948/DEGR
- Expert Insights
  - https://www.expertinsights.com/services/security-awareness-training/reviews

Phishing Attacks

Questions?

Weak Password/Authentication

Weak Password/Authentication

Statistics:

- 19% of employees
    - Use easily guessed passwords
    - Share passwords across accounts

Weak Password/Authentication

What is it?

Weak Password:

- Easily guessed or cracked password that can be quickly overcome by an adversary

Shared Passwords:

- Using the same password for multiple platforms

Weak Password/Authentication

Why is it difficult to defend against?

Human nature

- People will tend to use something as easy as possible for a password unless complexity rules are enforced
- People will tend reuse passwords
  - They may use the same password on a less secure site.

Weak Password/Authentication

What can you do?

- Multi-factor Authentication
  - Google Authenticator
    - https://support.google.com/accounts/answer/1066447?co=GENIE.Platform%3DAndroid&hl=en
  - Google Multi-Factor
    - https://www.google.com/landing/2step/
  - Microsoft Multi-Factor
    - https://support.microsoft.com/en-us/help/12408/microsoft-account-how-to-use-two-step-verification
- Password Management Platforms
  - https://www.expertinsights.com/services/business-password-management/reviews

Weak Password/Authentication

Questions?

Malware

Malware

Statistics:

From 2018 to 2019

- 350,000 Malware version identified every day
- New malware released every 7 seconds
-

Malware

What is it?

Malicious code that hackers create to gain access to networks, steal data, or destroy data on computers.

Malware usually comes from malicious website downloads, spam emails or from connecting to other infected machines or devices

Malware

Examples:

- **Viruses:** A harmful piece of code that enters your computer through being downloaded, or when you click a link. Viruses come in many shapes and forms and can have many effects on your device.
- **Spyware:** A particular kind of programme that enters your device (again, through being unintentionally downloaded or by you clicking on a bad link). Spyware watches what happens on your device and can capture information such as passwords or bank account numbers. It may also turn on your webcam and use this to watch what you type or to catch you doing something that might be embarrassing if others saw the video…
- **Ransomware:** Ransomware is a programme that enters your device (again, downloading, link clicking) and holds your device hostage. The programme will threaten to destroy your information unless you pay a ransom (which is generally in the form of Bitcoin nowadays, though it may be a wired amount of money).

Malware

Why is it difficult to defend against?

- I has many different implementations
- It is a constantly evolving threat
- Most modern malware is designed by and for professional criminals

Malware

What can you do?

- Personal vigilance,
- Products to filter for Malware
  - Network based
    - https://www.expertinsights.com/services/cloud-web-filtering/reviews
  - Endpoint based
    - https://www.techradar.com/news/best-endpoint-security-software

Questions?

Ransomware

Ransomware

Statistics:

- One of the most common cyber-attacks
- 71% of ransomware attacks targeted small businesses (More likely to pay ransom)
- Average Ransom demand? 116,000.00
- Most lucrative form of attack

Ransomware

What is it?

Ransomware involves encrypting company data so that it cannot be used or accessed, and then forcing the company to pay a ransom to unlock the data.

Ransomware

Why is it difficult to defend against?

- It is usually the end result of a combination of the other tactics used in this presentation
- Ex:
  - Phishing -> Malware -> Ransomware
  - Weak Passwords -> Ransomware
  - Insider Threat -> Ransomware

Ransomware

What can you do?

- Start with using best practices in the other sections of this presentation
- IMPORTANT: Your best defense against a ransomware attack is to have a through backup strategy in place

Ransomware

Questions?

Social Media

Social Media

What is it

- Social media is an important part of your business’s online image and advertising.
- Social media allows you to interact directly with customers from around the world

Social Media

Common threats

- Hacked accounts
- Stolen passwords
- Brand impersonation
- Uncontrolled user and account access

Social Media

Hacked accounts

- Can use your brand to spreading malware and scams to your customer base
- Loss of trust in the brand can result

What to do:

- Keep a close eye on when/where your account is logged into

Social Media

Stolen passwords

- Can allow a criminal full access to your account

What to so:

- Never use the same passwords on private and business profiles
- Don’t let unauthorized users log into your social media profiles

Social Media

Brand impersonation

- Attacker attempts to impersonate a trusted brand or personality (makes a copy of your profile)

What to do

- Report them to the site you’re using
- Post a warning to your followers.

Social Media

Uncontrolled user and account access

- Current employees who don’t need access to your account to do their job
- Former employees who may still have access

What to do

- Keep the number of users small and manageable
- Have a system in place for employees that are leaving

Social Media

Questions?

MATC Programs

For more information on Madison Colleges Cyber Security of other Information Technology programs.

- http://itins4.madisoncollege.edu/IT/programs.html

For more information on Madison Colleges Agricultural Equipment Program.

- https://madisoncollege.edu/program/agricultural-equipment-technology

Presenters contact Information

Mike Masino

- mmasino@madisoncollege.edu

Denny Wright

- dwright2@madisoncollege.edu