COMPUTER SECURITY AWARENESS

Karen LaPlant & Sheri Hutchinson
MN Summit on Learning & Technology
August 1, 2019

Participants will:

- Learn computer security basics.
- Share security tips.
- Give users the information they need to understand the nature of the threats they face.

PURPOSE

Learn simple things that you can do to secure:

Your Data

Your Computer

YOU

Users are Weak Link

Users are the weak link in your network security.
User training is a best practice to bolster cyber defense.

Educate Users

Educate users and help them understand the critical role they play in preventing data breaches. When developing a **COMPUTER SECURITY AWARENESS TRAINING**, lay a strong foundation by covering the basics first.

Keep It Simple

Keep it simple; give users the information they need to understand the increasingly sophisticated nature of the threats they face.

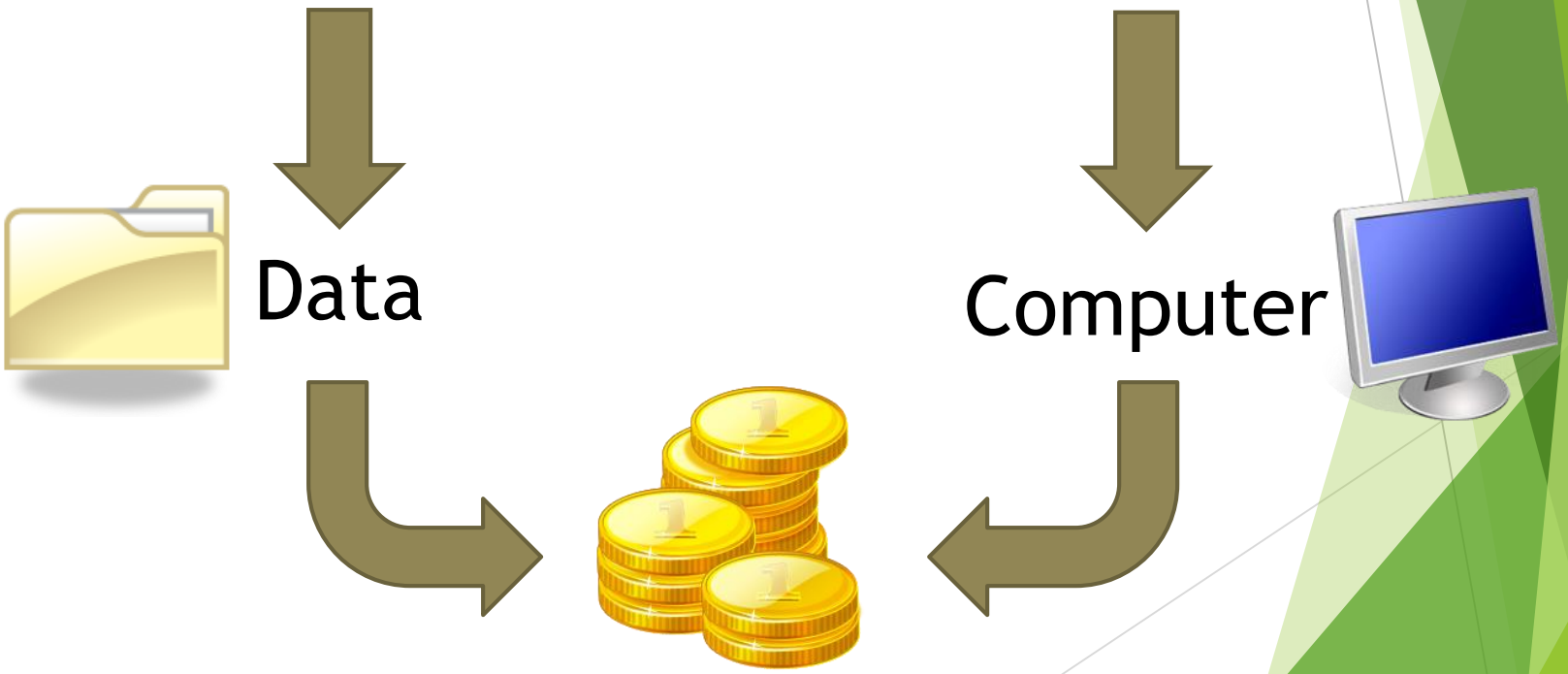
TOPICS

- You are the Target
- Social Engineering
- Email & Messaging
- Browsing & Malware
- Social Networks
- Mobile Device Security
- Passwords
- Data Security
- Report an IT Security Incident

YOU ARE THE TARGET

THE NEED FOR IT SECURITY

You have things attackers want.



VALUABLE ITEMS

Financial Records

Research Data

Classified Contract Information

Credit Card Numbers

SSNs

Grades

Student Records

Library Journals

Advanced Curriculum

Attackers can use YOUR Computer to gain **more** access and attack **further** into the Institutions.

Attacker

Blocked

Firewall

Your Computer

Server & Data

INCIDENTS ARE NOT UNCOMMON

TARGET

$248m

THE HOME DEPOT

$62m

Neiman Marcus

$4m

T.J.maxx

$118m

JPMorganChase

SONY PICTURES

UNIVERSITY OF MARYLAND 18 56

NORTH DAKOTA UNIVERSITY SYSTEM

ACCESS. INNOVATION. EXCELLENCE.

THE NEED FOR SECURITY

- Data breaches **can** happen here.
- They can cause devastating results: financial **and** reputational.
- **You** are the target and **You** can help prevent them!

SOCIAL ENGINEERING

The clever manipulation of the natural human tendency to trust.

SOCIAL ENGINEERING

- Asking for information they should not have access to
- Using confusing or technical terms
- Creating a sense of urgency

EMAIL AND MESSAGING

WHY EMAIL?

Email (and messaging) attacks are a **primary source** of breaches & compromised accounts.

Attacks are virtually free.

Attacks are simple and easy.

Lack of security in Internet email systems.

EMAIL ATTACK TYPES

Phishing Sending unsolicited emails looking for passwords and unprotected computers

Spear Phishing Using personal or custom messages in Phishing attacks

Whaling Sending Spear Phishing attacks to executives and management

EMAIL ATTACKS WORK

HVAC subcontractor fell victim to a Phishing attack

Internal employee phished, resulting in stolen security keys

HOW EMAIL ATTACKS WORK

Email attacks **require action** from the victim to work.

Opening an Attachment	**Success**
• Attachment runs a virus	9%

Clicking a Link	
• Attacker asks for password	9%
• Attacker sends virus thru browser	18%

SUSPICIOUS EMAIL

From: Sidney Cole [mailto:scole@jths.org]
Subject: HELPDESK

Your mailbox is almost full.

1961MB	**2048**MB

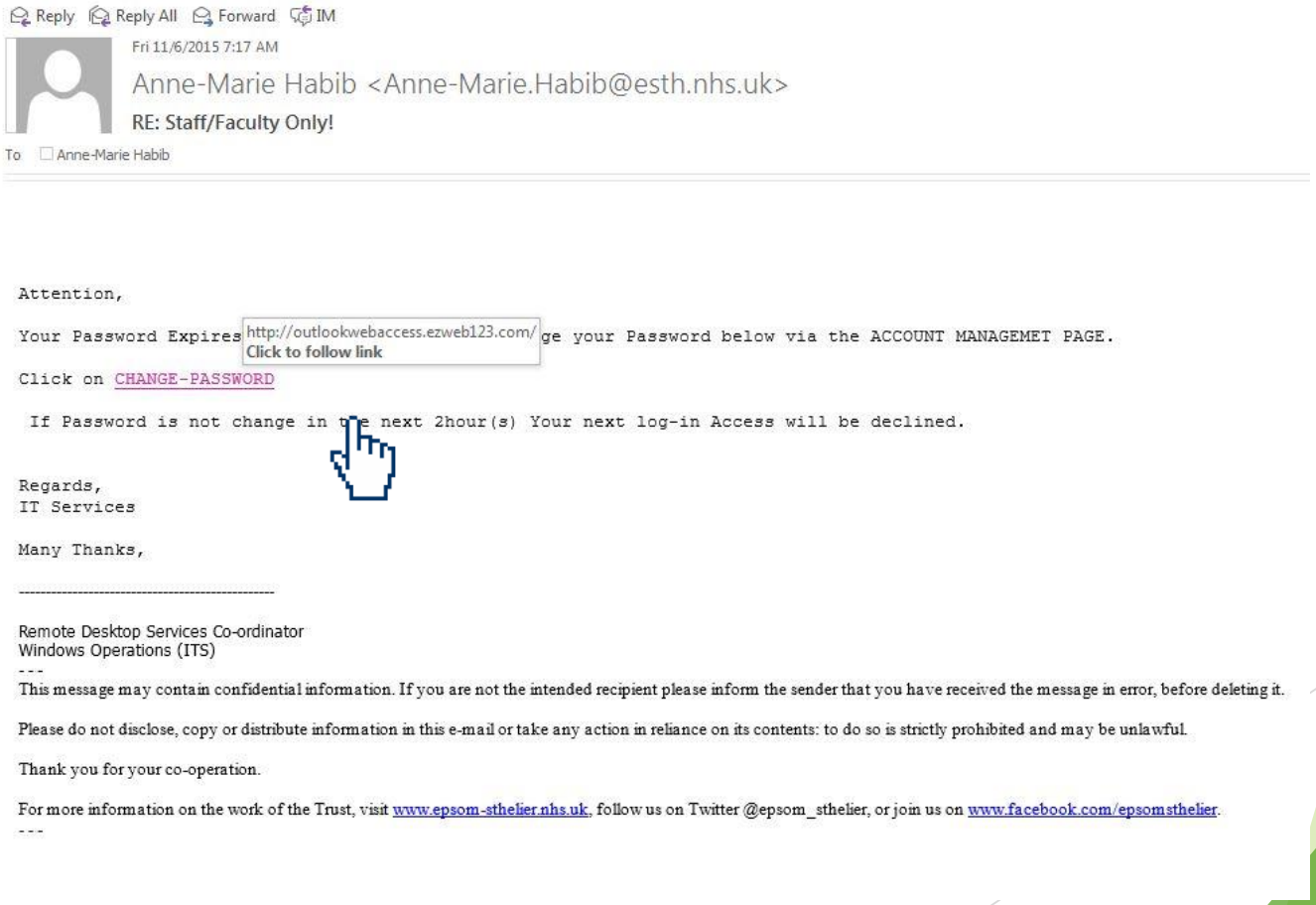
Your e-mail account will expire today. CLICK HERE www.badbadsite.com to validate your current password and Increase Your mail-box account QUOTA SIZE to our new outlook web.

Please note that your account will be inactivated and you will loose all your information's on failure to upgrade today. You are not required to change your password after this upgrade and upgrade is completed once redirected to Google. Thanks.

IT-service Desk.

HOVERING

Hover your mouse over your email links to see where it actually takes you.



EASY PREVENTION

Only click links or open email attachments that are **expected** and from **trusted** individuals.

Watch for poor **spelling**, **grammar**, and excessive **capital letters**.

Don’t implicitly trust the “**From**” field – it can easily be forged.

MORE PREVENTION TIPS

Emails warning of a **locked account** or a **full mailbox** are common scams.

If an email is “fishy”, get **confirmation** it is legitimate thru other means.

When in doubt, **throw it out!**

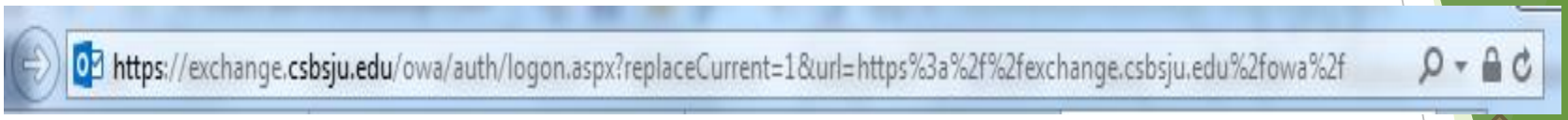
BROWSING & MALWARE

BROWSING BEST PRACTICES

- If you see a warning against visiting a site, don’t connect to it.
- Keep your browser current.
- Do not install plugins or add-ons.
- Scan files that you download with anti-virus software.

PADLOCK IS GOOD

A padlock before or after your URL indicates it is safe and has been verified.



Check for this when typing in your username and password on sites.

If you are ever unsure where a link will go, type it in manually.

WHAT IS MALWARE?

Malicious software **(malware)** is used to describe a variety of bad things:

Viruses Worms Ransomware

Trojan Horses Spyware

HOW BAD COULD IT BE?

Malware is so **sophisticated** many times it is **impossible** to remove it without formatting the entire computer.

The Cryptolocker malware **encrypts** the files on your servers and desktop and **extorts** you if you want your data back.

MALWARE SOURCES

Attackers use malware to steal our data and our computer resources.

Malware can come from:

- Email Attachments
- USB (flash) Drives
- Misconfigured Servers
- Trusted & Untrusted Websites

MALWARE SOURCES

Malware can spread thru USB sticks.

Common tactic is to “drop” them and wait for someone to plug it in.
Don’t try unknown flash drives.

Also via “Traditional Hacking”.
Exploits thru vulnerabilities.
Keep computers patched.

WEBSITE MALWARE

A **drive-by malware attack** happens when malware is sent to your browser during your normal Internet use.

Takes advantage of **old** and **unpatched** software such as Java and Flash.

Happens **silently** and can occur while browsing **legitimate** sites.

WEB MALWARE PROTECTIONS

- **Watch** what you click.
- Don’t visit risky websites.
- Run an antivirus program on your computer.
- Keep your software up-to-date.

COMBATING MALICIOUS SOFTWARE

- Many Different Types of Malware
- Malware Comes From USB Sticks & Websites
- Good Malware Protections
- Call For Help if Infected

SOCIAL NETWORKS

SOCIAL NETWORK - RISKS

- Stolen identity.
- Privacy controls can be confusing and change.

PROTECT YOURSELF

- Information will become PUBLIC.
- If you don’t want your boss, co-workers or family to see information – DO NOT POST IT
- Watch what others post about YOU.

CYBER ATTACKS

- Hack into your account.
- Confirm suspicious messages.
- Be cautious about third-party applications.

MOBILE DEVICE SECURITY

KEEP YOUR PHONES SAFE

Four Easy Security Tips

(Whether you have sensitive work data or not)

Use a Passcode or Fingerprint ID

Set Device to Auto Lock

Do not “Jailbreak” your Device

Enable Remote Tracking

PASSWORDS

PASSWORDS ARE PAINFUL

We all have many passwords, associated with various accounts, applications and sites.

PASSWORD SCHEME

Create a passphrase

Example: My 3rd Cousin, Chews Bubblegum!!

Create a password pattern

Base: **Ch0p$ticks**

Electric: **Ch0p$ticksZAP**

Apple ID: **iCh0p$ticks**

Don’t make it too predictable.

PASSWORD TIPS

Keep your account safe by **never** doing:

- **Never share** your password with anyone.
- **Never talk** about your password.
- **Never reveal** your password on questionnaires, surveys or emails.
- **Never write down** your passwords and store them by your computer.
- **Never save** passwords in your browser.
- **Never reuse** a password between sites.

SAFEGUARDING YOUR CREDENTIALS

- Your network account is the gateway to all of your data.
- Use Strong Passwords.
- **NEVER** Share Passwords.

DATA SECURITY

MAKE IT A HABIT

Why lock your computer when getting a printout or visiting the bathroom?

Offices are in semi-public buildings
Unexpected diversions

It's easy!

- Windows: +L
- Mac: Configure screen corner

ADDITIONAL SECURITY

In under a minute, an attacker could:

- Alter records in ISRS.
- Send a fraudulent email.
- Exfiltrate sensitive documents.
- Install a keyboard sniffer.

- **Keep** sensitive paper files stored.
- **Lock** computers when not in front of them. Your office is your kingdom.

REPORTING AN INCIDENT

SIGNS OF COMPROMISE

- Anti-virus alerts.
- Browser redirecting to random sites and you are unable to close it.
- Passwords no longer work.
- Messages being sent from you that you did not send.
- Installation of suspicious software.

REPORTING AN INCIDENT

If you think your computer is infected with malware, contact the IT Help Desk ASAP.

Don’t feel embarrassed or discount it as unimportant.

For immediate help, please call the IT Help Desk on campus, dial 1411 or submit an online work ticket.

CONCLUDING TODAY'S SESSION

- **You are the Target**

Data breaches happen and attackers want your data.

- **Social Engineering**

Tricking you into believing that you should give information or install applications.

- **Email & Messaging**

Phishing is not going away; identify telltale signs. Verify links & messages and report attacks.

CONCLUDING TODAY'S SESSION

- **Browsing & Malware**

  Watch where you browse and click; keep your software up-to-date. Malware comes in many flavors from USB sticks, emails, and websites.

- **Social Networks**

  Be careful what you post online.

- **Mobile Device Security**

  Protect your mobile device. Lock, encrypt and keep track of it.

CONCLUDING TODAY'S SESSION

- **Passwords**
  Passwords are important, so never share them! Use strong passwords to stay secure.

- **Data Security**
  Lock your computer and protect your mobile devices.

- **Reporting an Incident**

  Contact IT Services Help Desk for suspected incidents.

10 Tips To Stay Safe

- Install software updates
- Use unique passwords
- Use 2-factor authentication
- Use strong passwords
- Use password manager
- Change passwords
- Do not share info
- Resist Phishing
- Personal Computer Defenses
- Mobile Defenses

SUMMARY

Remember 3 Simple Rules to Stay Safe Online

- Stop-Look-Think
  - Hit that delete key!
- Spot a Red Flag?
  - Try to verify suspicious email
- When in doubt, report and throw it out!

There are a thousand ways that internet criminals will try to scam you, and only 1 way to stay safe.

Stay Alert as you are the last line of defense!

Thank you for attending today's session of

Computer Security Awareness

Your participation and support **keeps us all safe.**

CONTACT US:

Karen LaPlant

Karen.LaPlant@metrostate.edu

Sheri Hutchinson

Sheri.Hutchinson@minnstate.edu