Data Security & Privacy

Purpose

- Basic awareness of data security and privacy best practices
- Notification to the local board that the district has reviewed and implemented best practices

702 KAR 1:170

- Requires that the district acknowledge to its local board prior to August 31 of each year that it has reviewed the guidance of the KAR and implemented best practices

Relevant Board Policies & Procedures

- 01.61 – Records Management
- 01.61 AP.11 – Notice of Security Breach
- 09.14 – Student Records

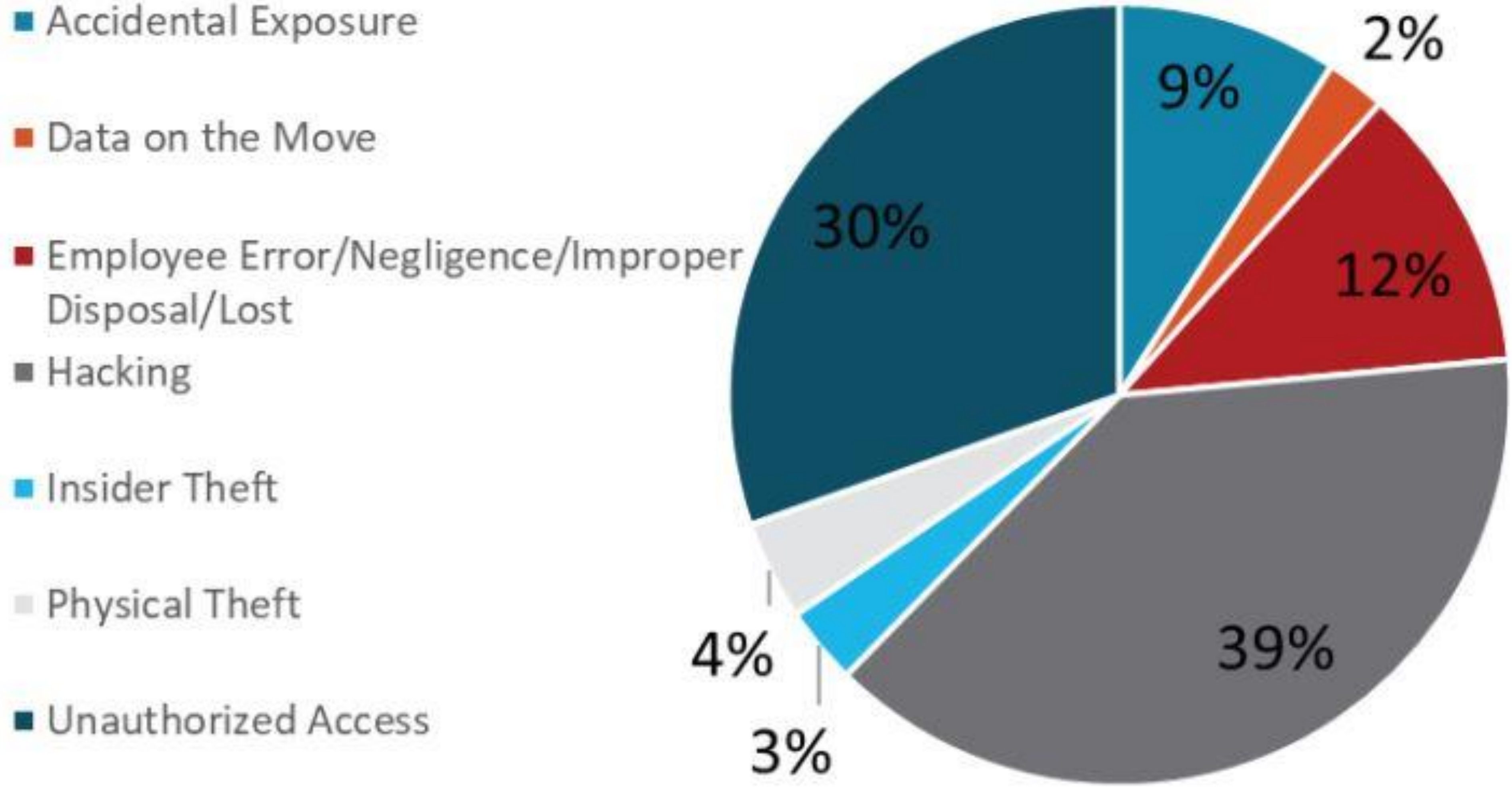
Data Security Implementation Plan

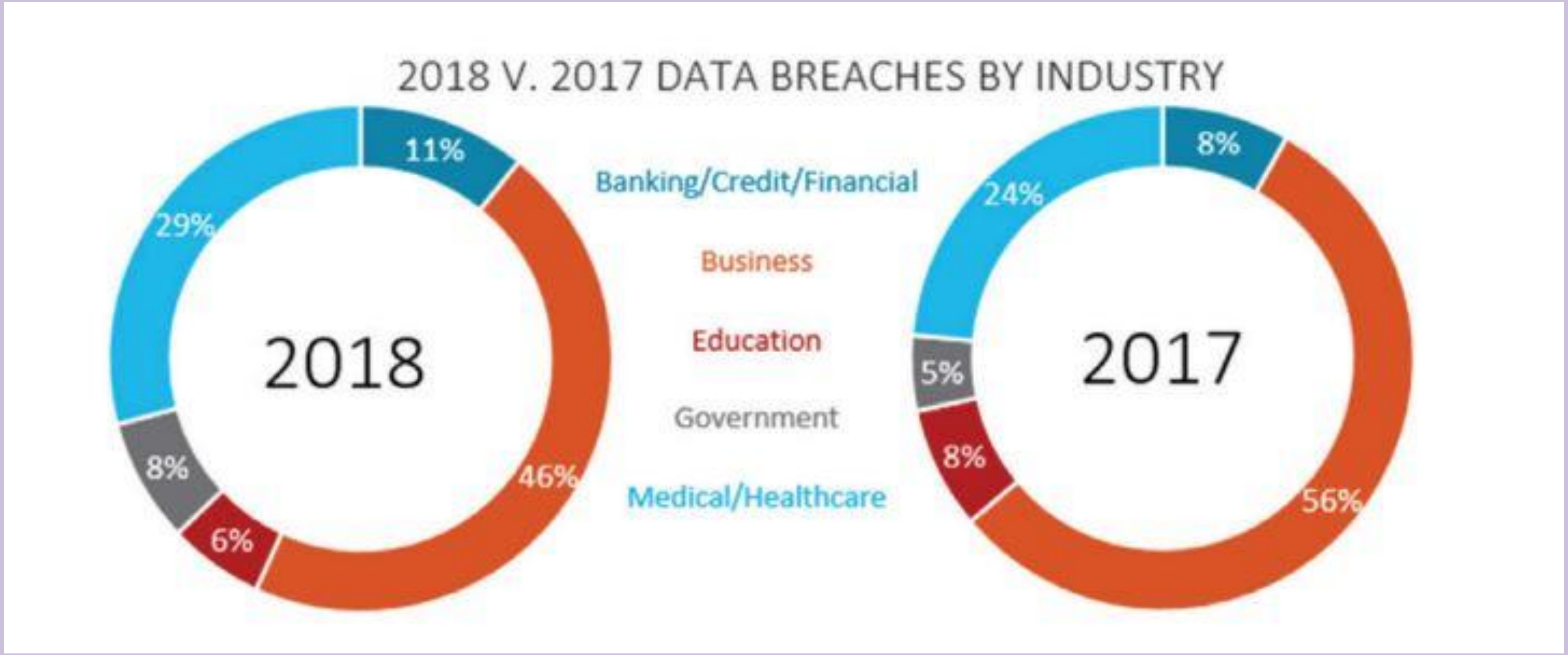
- Identify and document data (both electronic and hardcopy) that need to be protected
- Audit current access to data by various groups of people and make adjustments as needed
- Document data security measures and security breach procedures
- Provide awareness training with all staff who have access to confidential data

Main Causes of Data Breaches

- Human Error
  - Accidental sharing (email, website, paper, etc.)
  - Weak or stolen passwords
  - Loss or theft of employee device (USB drive, laptop…)
  - Phishing, clickbait
- Everything Else
  - Application vulnerabilities – unpatched software
  - Hackers
  - Malware

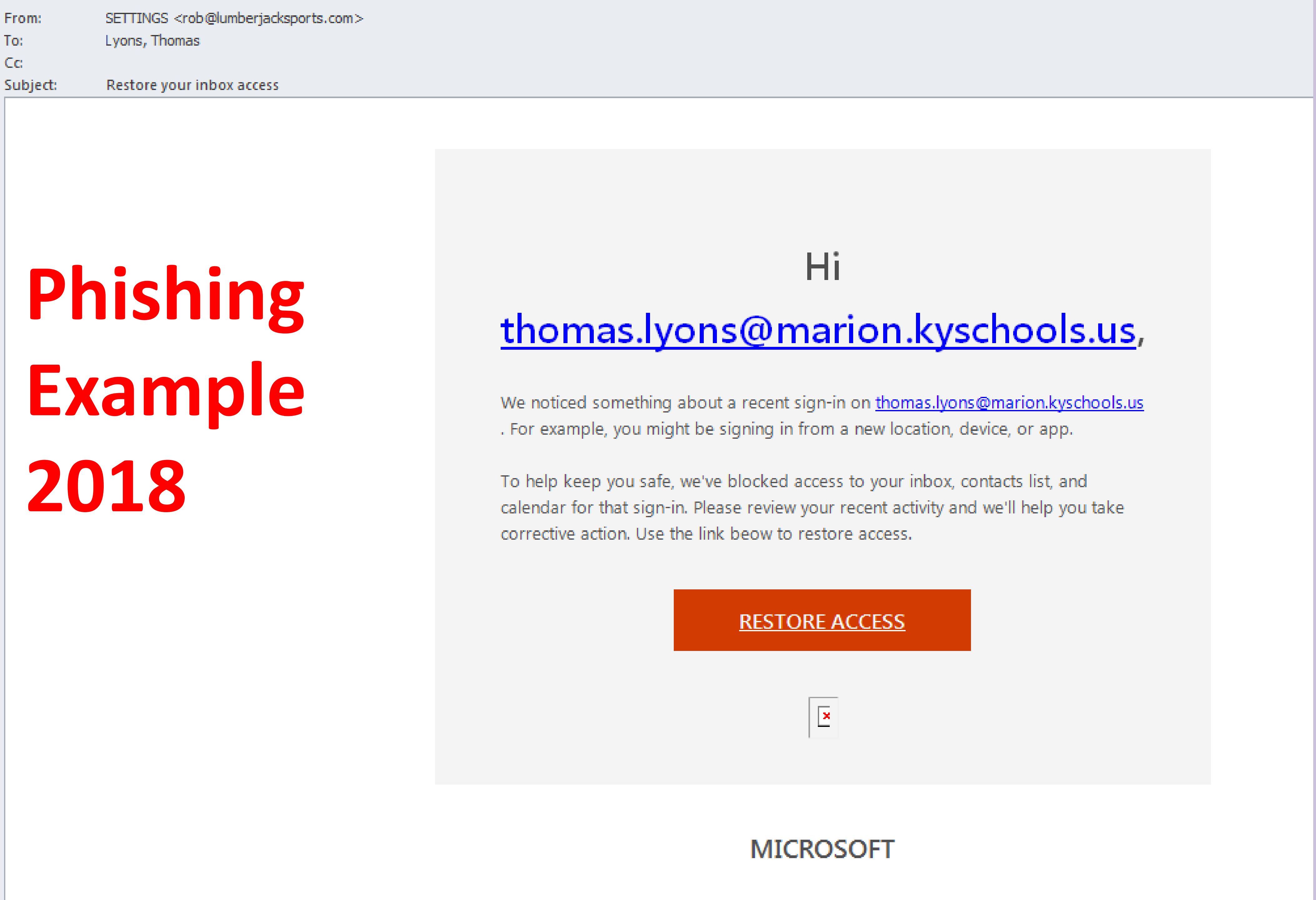
2018 BREACHES BY TYPE





Graphic via
Identity Theft Resource Center

Phishing Example 2018



From: SETTINGS <rob@lumberjacksports.com>
To: Lyons, Thomas
Cc:
Subject: Restore your inbox access

Hi thomas.lyons@marion.kyschools.us,

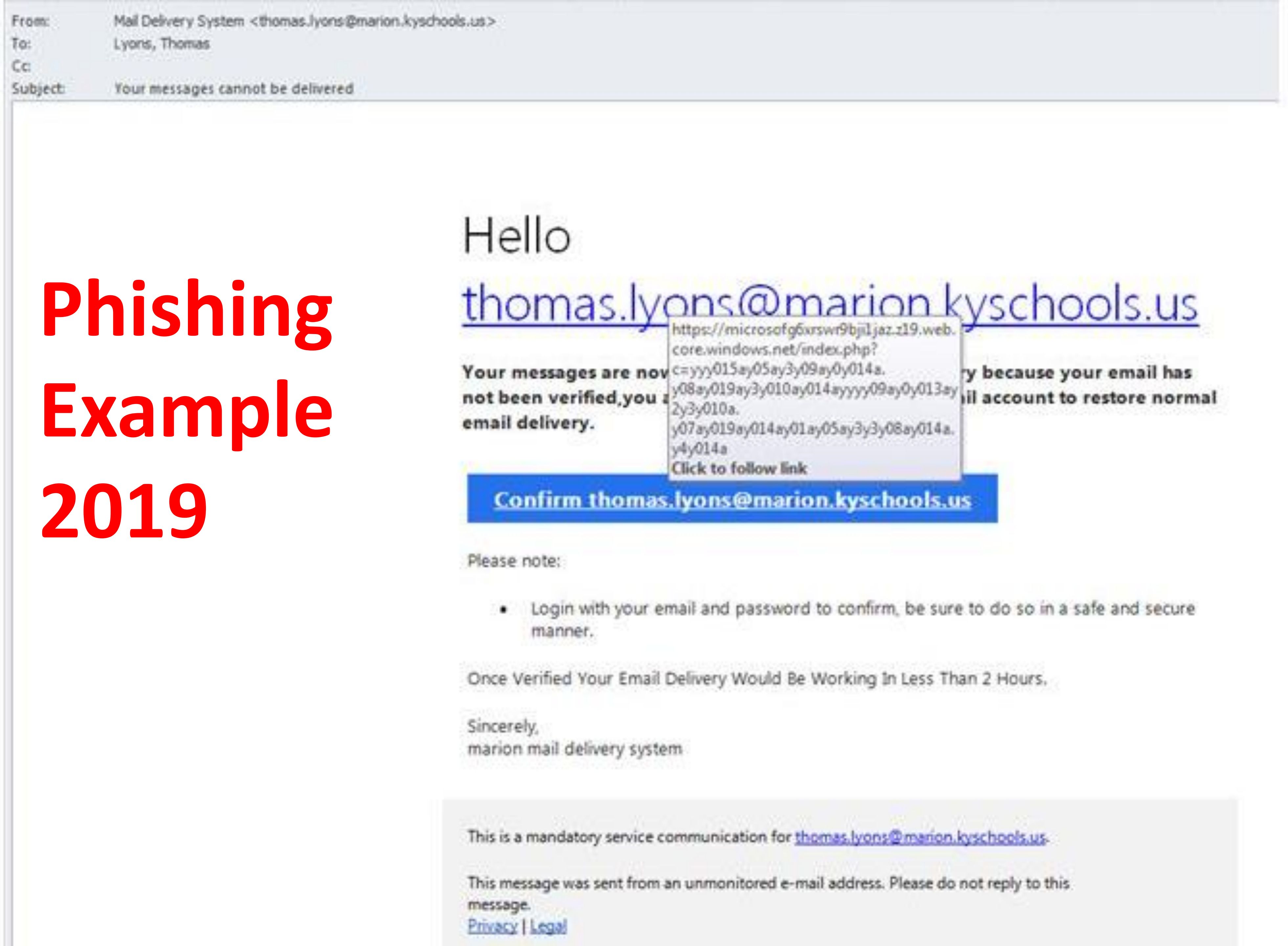
We noticed something about a recent sign-in on thomas.lyons@marion.kyschools.us . For example, you might be signing in from a new location, device, or app.

To help keep you safe, we've blocked access to your inbox, contacts list, and calendar for that sign-in. Please review your recent activity and we'll help you take corrective action. Use the link beow to restore access.

RESTORE ACCESS

MICROSOFT

Phishing Example 2019



From: Mail Delivery System <thomas.lyons@marion.kyschools.us>
To: Lyons, Thomas
Cc:
Subject: Your messages cannot be delivered

Hello

thomas.lyons@marion.kyschools.us

https://microsofg6xrswr9bjil1jaz.z19.web.core.windows.net/index.php?c=yyy015ay05ay3y09ay0y014a.y08ay019ay3y010ay014ayyyy09ay0y013ay2y3y010a.y07ay019ay014ay01ay05ay3y3y08ay014a.y4y014a
Click to follow link

Your messages are nov ry because your email has
not been verified,you a il account to restore normal
email delivery.

Confirm thomas.lyons@marion.kyschools.us

Please note:

- Login with your email and password to confirm, be sure to do so in a safe and secure manner.

Once Verified Your Email Delivery Would Be Working In Less Than 2 Hours.

Sincerely,
marion mail delivery system

This is a mandatory service communication for thomas.lyons@marion.kyschools.us.

This message was sent from an unmonitored e-mail address. Please do not reply to this message.
Privacy | Legal

Confidential Data

- Student education records except “directory” information in certain circumstances
- PII (Personally Identifying Information) as defined by FERPA and House Bill 5

Security Breach Notification

Notify all individuals and agencies as outlined in KRS 61.933 if PII has been disclosed and will result in the likelihood of harm to one or more persons

One of these

- First name or first initial and last name
- Personal mark
- Unique biometric print/image

AND

One or more of these

- Account number with PIN that would allow access to the account
- Social Security Number
- Taxpayer ID number
- Driver's license number or other ID number issued by any agency (student ID number)
- Passport number or other number issued by the US
- Individually identifiable health information except for education records covered by FERPA

Current Measures to Prevent a Breach

- Anti-Virus/Malware/Spam/Spyware Protection
- Vulnerability Scanning
- System Patch Management
- Cloud/Offsite Resources
- Active Directory/Group Policy Objects
- Private IP implementation
- Distributed Denial of Service (DDOS) Mitigation
- Web Filtration
- Centrally Managed Firewalls
- Virtual Private Network Support
- Secure File Transfer
- Private Printing
- Statewide Product Standards
- Locked Data Center
- Locked File Cabinets/Doors
- Limited Access (Need to Know)
- Removal of user accounts for staff no longer employed
- Staff confidentiality and security training
- Video surveillance systems
- Strong password rotation

Student Data

- "Student data" means any information or material, in any medium or format, that concerns a student and is created or provided by the student in the course of the student's use of cloud computing services, or by an agent or employee of the educational institution in connection with the cloud computing services. Student data includes the student's name, email address, email messages, postal address, phone number, and any documents, photos, or unique identifiers relating to the student. (KRS 365.734)

Cloud Providers

- KRS 365.734 prohibits cloud providers from processing student data for any purpose other that improving its services. Specifically prohibits use of data for advertising and selling of student data.
- Current cloud providers/programs: Infinite Campus, Pearson, NWEA (MAP), Google, Microsoft, AIMS Web, KET Encyclomedia, Edmodo, MobyMax, Study Island, Khan Academy, Edmentum, Read 180, BrainPOP, Renaissance Learning, Follett, Starfall, Schoolology, Naiku, Lifetouch, Prezi…

Questions?