Safe Computing Practices
Phishing
What is Phishing

- Malicious emails used to gather information.
- Malicious emails used to launch further attacks
- Malicious emails used to lure a victim into giving up sensitive information (passwords, payment card data, Government ID’s)
- Malicious emails which may deliver viruses or other malware.
- A form of social engineering.

Stop the Phish!
Phishing Example 1 - Red Flags

From: [mailto:karen_campbell@middlebury.edu]
Sent: Wednesday, February 10, 2016 1:11 PM
To: [mailto:mark@middlebury.edu]
Subject: Employees Wage Data

Hello Mark,

I need a comprehensive information of all employees' wage information.

Could you put them together in E-copies/format (preferably all employees' 2015 W2s) and write back attaching the copies or file to the message. I need the wage data after tax and other deductions for review.

Thank you,

Karen Campbell
Director, Payroll

While this address looks like it will go to a Middlebury address, security systems reveal that this email will reply to a malicious email of CPA@gormicpa.com.

Always watch for emails with unreasonable requests or content that does seams out of character.

Knowing the sender does not make the email reputable.
Phishing Example 2 – Spoofed Senders

Emails sent from a compromised @middlebury.edu email account!

From: [Redacted]
Sent: Tuesday, June 16, 2015 5:28 PM
Subject: Middlebury :- 1 New Message

To Middlebury Faculty, Staff & Students:

You Have 1 New message.

Click Here To Read

Regards,

Middlebury College

© 2015 Middlebury College. All Rights Reserved.

[Hover Over]

From: [Redacted]
Sent: Tuesday, June 16, 2015 5:28 PM
Subject: Middlebury :- 1 New Message

To Middlebury Faculty, Staff & Students:

You Have 1 New message.

[Click to follow link]

Click Here To Read

Regards,

Middlebury College

© 2015 Middlebury College. All Rights Reserved.
XXXX,

Are you at your desk?
Process a wire transfer of $49,780.00 to the attached account information.

This payment should be coded to ‘Operating Expenses’.

I’ll expect you to get it done by COB today. Send me a note immediately payment is completed.

Thanks,
Phishing Example 4 - Malicious Attachment

From: Theresa Gleason [mailto:theresachancegleason@gmail.com]
Sent: Wednesday, May 25, 2016 12:24 PM
Subject: File

Google Drive

Theresa used Google drive to share Secured File with you securely!

View — Download files

scan011.pdf

scan012.pdf
Phishing: Caution Signs

• If it is in your Quarantine
  use extra CAUTION!

• If it is in your Junk Email
  use extra CAUTION!

• If it has obvious or uncharacteristic
  grammar and spelling errors
  use extra CAUTION!

Thanks i waiting your email to me

phishing@middlebury.edu
SCAMS to Watch For:

- **Credit Card or Bank Scams**: Often mimic common banks and card companies trying to entice a potential card folder to expose their user credentials or account information.

- **PayPal Scams**: Have become increasingly prevalent from fake offers of PayPal benefits to scams around account information. The goal of these is always to elicit account credentials.

- **C-Level Scams**: Attackers have increased their efforts targeting C-Level or management level individuals. These attacks often are singular in their target (spear phishing) and extremely well crafted.

- **Tax/IRS Scams**: Most common around the New Year and tax season, these scams come in many forms to entice the victim to expose sensitive data such as social security numbers.

Justifications for Phishing attacks against:

- EDU Institutions have large financial resources.
- EDU Institutions have large and numerous technology resources.
- EDU Institutions have large numbers of targets often with little technical background.
- The United States has traditionally been a large target globally.
- Phishing has traditionally been one of the three most common cyber attack vectors.
- **Political and financial targets** are the majority of the cyber attack victims. EDU Institutions provide both of these targets in one location.

- **Middlebury has a large financial component** from tuition, donations, and the retail operations on campus.
- **Middlebury has a large political component** with both its reputation and the work done at MIIS.
Discussion and Links

Please share your thoughts!

Information Security Resources:
http://go.middlebury.edu/infosec
http://go.miis.edu/infosec
http://go.middlebury.edu/infosecfeedback

Report Information Security Events To: infosec@middlebury.edu