1. Intro and Welcome – Bob Nakles

2. Updates from the CIO – Marilyn
   - The new ITS
   - "Security: It's Everyone's Job" and the need to communicate within departments
   - Monthly newsletters – SL's need to share with their department
   - Ask questions of the ITS, no need to wait for a meeting
   - Recent events, the APT and the web event

3. Phishing- Karen Bates
   - Video clip
   - Recent or common phishing emails
   - How to tell if an email is legit

4. IT Security Projects – Curtis McNay
   - The list of proposed or current projects related to security

5. Review the role of the SL - Bob
THE CIO’S UPDATES

Updates from the CIO – Marilyn T. Smith

❖ The new ITS

❖ "Security: It's Everyone's Job" and the need to communicate within departments

❖ Monthly newsletters – share with your department

❖ Contact the ITS, no need to wait for a meeting

❖ Recent cyber security events
PHISHING

Karen Bates

- Video clip: How easy it is to get a person’s credentials
- Examples of recent and common phishing emails
- How to tell if it’s legit
COMMON PHISHING EMAILS
How hard is it to get passwords?

https://www.youtube.com/watch?v=opRMrEfAliI
From: University Employment Portal <info@gmuemploy.org>
Sent: Friday, November 28, 2014 10:06 AM
To: jaladig
Subject: Part Time Job Opening

Hello,
Do you want to work part time, 30 minutes daily, as a correspondent payroll officer for a Chinese Art & Craft company? Can you handle money matters properly without mistakes? If YES, then this job is yours, apply now to get it!! Payment is $250 weekly (i.e. $1,000 monthly) The employer's direct email has been attached to this ad, hence respond only if you are interested.

Thank you,
Huang Gong
Employment Bureau
University Employment Portal
This ad is FERPA protected under US Laws

---

George Mason University uses a different email address

There is no business name, no university name, address or contact information

Should be arts and crafts and the question mark is off

Hence is a word rarely used today

Punctuation is incorrect. There should be a period after yours. Apply should start a new sentence

There should be a period after yours.
Mason will not have a person from another university send you information about your expired password.

Your Password will Expire 3 days Click Here (http://hjhhghgdghhg.wc.lt/) to update your account.

- Vague information and improper salutation
- Uppercase letters used improperly and no punctuation
- This link actually goes to a site in the United Kingdom
From: System Administrator <wramsey@hazlet.org>
Sent: Tuesday, November 4, 2014 3:03 PM
Subject: Attention: E-mail User

Attention: E-mail User,
Your mailbox is almost full.
254MB  250MB
Current size   Maximum size

You have exceeded your E-mail account limit quota of 250MB and you are requested to increase/expand it within 24 hours and avoid disability of your e-mail account from our database. Simply CLICK HERE and complete the information requested to automatically expand your account quota to 2 GB.
From: <Eyrich>, Jeanine <jeanine.eyrich@Vanderbilt.Edu>
Date: Thursday, November 20, 2014 at 12:10 PM,
To: “Eyrich, Jeanine” <jeanine.eyrich@Vanderbilt.Edu>,
Subject: RE: FACULTY/STAFF/EMPLOYEE,
Resent-From: <saircmg@tntech.edu>
Resent-Date: Thursday, November 20, 2014 at 12:19 PM

Dear Webmail Subscriber,
Your Email Account have been Suspended from sending and receiving email, to re-validate your account, please,
CLICK HERE TO LOGIN USING SECURE ENCRYPTION

Connected to Microsoft Exchange
© 2014 Microsoft Corporation. All rights reserved
Microsoft Outlook Web App

Security (show explanation)

- This is a public or shared computer
- This is a private computer

Use the light version of Outlook Web App

User name

Email Address

Password:

Sign in

Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.
IT SECURITY PROGRAMS

Presented by Curtis McNay
Ø IT SECURITY - REALMS OF OPERATION

**Proactive**
- Policy
- Inventory, Classification
- Risk Assessment
- Access Control
- Active Blocking
- Vulnerability Detection
- Network Architecture
- System Hardening
- Awareness & Training

**Reactive**
- Network & System Monitoring
- User & Data Monitoring
- Application Monitoring
- Threat Analysis
- Gap Analysis
- Incident Response
- Data and System Recovery
PROJECTS - PROACTIVE

➢ IT-GRC - Inventory, Classification and Assessment
  ❖ Inventory & classify systems and applications & check for vulnerability.
  ❖ Identifies critical system for focus.

➢ Multifactor Authentication – Provides Access Control security
  ❖ Could have prevented hackers from getting into network and on to privileged systems.

➢ NextGen IPS - Network Intrusion Protection System
  ❖ Could have blocked Remote Access Trojans (RATs), BOT sessions & reconnaissance.

➢ Vulnerability Scanning - Upgrade of active & passive scanners & GRC integration
  ❖ Identifies Vulnerabilities, and with authenticated scans, misconfiguration.

➢ Web Application Firewall – F5 Security Module
  ❖ Could have prevented Web application compromises.
IT Security Awareness and Training – Says it all.
- General awareness and role specific training, from phishing to database security.

Local Controls for Windows systems - Restrict Built-in Admin & limit local log in
- Secure the built-in admin. And limit access to the people that need access.

IronPort Upgrade and Optimization – Protection from Phish
- Goal of reducing the number of and improving the alerting for phishing email.

Application Whitelisting for Critical Servers – Malware protection
- Could have prevented or alerted to malware on critical servers.

Prohibit Unnecessary Server to Server communication - contains infections
- Could have limited penetration by APT attackers.
ArcSight Upgrade, Expansion and Analysis - Better performance, more log sources, longer retention. Maturing correlation for more meaningful data
  - Provides monitoring, alerting and threat analysis
  - Provided active attacker forensics during APT.

F5 Web Application Monitoring – Threat analysis for Web applications
  - Identifies threats to and gaps in web application security.

Next Gen IDS - Intrusion Detection Monitoring
  - Increased Visibility of Malicious Network traffic.

CSIRT Lessons Learned-
  - How did it happen & What do we do differently.

Disaster Recovery Tabletop Exercise
  - To improve CSIRT and Communication,
YOUR ROLE

Bob Nakles

Provide security updates to staff
  Newsletters, monthly
  Email notifications, such as the recent reminder of phishing

Call for resources, presentations, information

Remind people to forward suspected phishing to the Support Center support@gmu.edu
YOUR RESOURCES

Resources

IT Security Office information
Cyber Security Month activities (October)
Online resources

http://itsecurity.gmu.edu/SecurityLiaisons/about-liaisons.cfm

http://itsecurity.gmu.edu/Alerts/Advisories.cfm

http://itservices.gmu.edu/alerts/