UCF Faculty Senate
Information Technology Committee

Minutes of **March 16, 2020**
Via Zoom

Melanie Guldi, chair, called the meeting to order at 2:04 pm. The roll was called orally.

In Attendance: Anya Andrews, Dawn Eckhoff, Sandra Galura, Steffen Guenzel, Melanie Guldi (Senate Liaison), Joseph Harrington (Steering Liaison), Athena Hoeppner, Pieter Kik, Viatchelslav Kokoouline, Robert Macy, Heath Martin, Matthew Nobles, Michael Sink (ex officio), and Francisca Yonekura (ex officio).

Minutes: Motion and second made to approve the minutes of the February 17, 2020 meeting. The minutes were approved. Motion and second made to approve the minutes of the March 2, 2020 meeting. The minutes were approved.

Chair Announcements:

- The chair invited guest Chris Vakhordjian from Information Security Office; due to the rapid switch to remote work/remote learning Michael Sink and Chris Vakhordjian were late to the meeting.
- The chair highlighted information regarding the planned phase-out of IMAP and POP that Chris Vakhordjian from Information Security Office provided since the March 2, 2020 meeting:
  - See the attached pdf: ISO Response on IMAP, POP and E-mail forwarding.pdf
  - Additionally, Chris V. emailed the information below:

    FBI Warns of BEC Attacks Abusing Microsoft Office 365, Google G Suite
    BleepingComputer, 6 Mar 2020: The FBI warned private industry partners of threat actors abusing Microsoft Office 365 and Google G Suite as part of Business Email Compromise (BEC) attacks. "The scams are initiated through specifically developed phish kits designed to mimic the cloud-based email services in order to compromise business email accounts and request or misdirect transfers of funds," the FBI said in a Private Industry Notification (PIN) from March 3. "Between January 2014 and October 2019, the Internet Crime Complaint Center (IC3) received complaints totaling over $2.1 billion in actual losses from BEC scams targeting Microsoft Office 365 and Google G Suite." The cybercriminals move to cloud-based email services matches organizations' migration to the same services from on-premises email systems. Targets are redirected to the phishing kits used as part of these BEC attacks via large scale phishing campaigns, with the phishing kits being email service-aware and capable of detecting the "service associated with each set of compromised credentials." "Upon compromising victim email accounts, cybercriminals analyze the content to look for evidence of financial transactions," the FBI explains. The scammers will then impersonate employees of the now-compromised organizations or their business partners, attempting to redirect payments between them to bank accounts under the attackers' control.
    The FBI issued a number of defense recommendations IT admins can implement on their networks to prevent BEC attacks:
    • Prohibit automatic forwarding of email to external addresses.
    • Add an email banner to messages coming from outside your organization.

• Prohibit legacy email protocols such as POP, IMAP, and SMTP that can be used to circumvent multi-factor authentication.
• Ensure mailbox logon and settings changes are logged and retained for at least 90 days.
• Enable alerts for suspicious activity such as foreign logins.
• Enable security features that block malicious email such as anti-phishing and anti-spoofing policies.
• Configure Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication Reporting and Conformance (DMARC) to prevent spoofing and to validate email.
• Disable legacy account authentication.
End users can also take these measures to defend against BEC scammers:
• Enable multi-factor authentication for all email accounts.
• Verify all payment changes and transactions in-person or via a known telephone number.
• Educate employees about BEC scams, including preventative strategies such as how to identify phishing emails and how to respond to suspected compromises.

The FBI recommends BEC scam victims to file a complaint regardless of the amount they lost at BEC.IC3.gov.

- Regarding the March 2 discussion of retiree information for Knights Email account creation and use, JP forwarded a link to a succinct knowledge article put together by UCF IT. It covers some of the more common questions related to retiree email. He indicated that all feedback is welcome, and that in addition to the link below, the article is easily accessible by searching “retiree” or “retired” at it.ucf.edu in the “Search the Knowledge Base” box. Link: https://ucf.service-now.com/ucfit?id=kb_article&sys_id=8ec66d481b2b8c505cd6b912cd4bcbc1
    - The committee raised issues regarding forwarding of email (which can’t be done to another email address), and that the language is targeted for students/faculty and not specifically for retired faculty.
    - The committee suggested giving this issue to the union, who may have additional input. The support for retirees is inadequate, and one example highlighted a particular example where a retired faculty member was unable to reset a password due to a circular issue with the password reset.
- This broadened into a discussion of IT service, in general. Many on the committee raised issues with service, including that UCF IT is not great at communicating, in general, and perhaps more people should be working to improve ServiceNow.
    - Example raised: University rolled out Microsoft Teams, but there was no systematic training available in how to use it.
    - Additional issue raised: UCF IT only solves a problem after sending multiple messages after creating an initial ticket.
    - Additional issue raised: Committee members suggested that relatively straightforward tasks like adding researcher-specific software should be allowed (via granting the faculty member some administrative privileges on their computers).
    - Chris V. pointed the committee to https://infosec.ucf.edu/security-standards/ as a response to why individuals do not have administrative access.

        - Committee would like to see a report from UCF IT regarding how many tickets they receive, what is the time to first response, and what is the time to resolution.
        - One committee member indicated that departments are charged for each IT ticket, so this may create a conflict of interest (UCF IT wants to increase tickets to increase revenue; the incentive to solve the problem quickly is low).
        - Michael Sink and Chris Vakhordjian joined the meeting late. Michael Sink indicated that they are piloting a program that would hopefully address some of the issues with ServiceNow, and possibly response times with UCF IT. He asked for the ticket number of the committee member who had trouble getting an issue resolved without multiple follow ups.

- **Old Business**

    - We did not have a long discussion regarding support for desktop Linux other than email (documented and published access solutions to all campus services, like printing, wireless, wired, and email; user support for desktop Linux). However, a plugin for email was mentioned that seems to be working (OWL). And Joseph Harrington indicated that he would continue to work with UCF IT to work toward a solution.
    - We did not discuss the item: Support for research computing (cloud CPU services, cloud document services, continuity of research computing over funding gaps, STOKES financial model, research group system support).
    - We tabled our discussion of the Mission of the Committee and how we can function more efficiently (items carried over from last academic year)
        - Description of the committee is available on Faculty Senate page: http://facultysenate.ucf.edu/committees/IT_committee.asp

- **New Business**
    - The committee decided to postpone our discussion of “Draft Resolution 2019-2020-X Linux Access to IT Services” until the fall, with the intention that it can be discussed in the fall if there is not progress on Linux support.

Other Business
- None

ADJOURNMENT

The meeting adjourned at 3:22 pm.

Resolution 2019-2020-X Linux Access to IT Services

Whereas,

Linux is among the best operating systems for teaching students to control computers, both for programming and for operating-system-level tasks,

Linux is free of charge and runs on a wide variety of hardware, enabling low- and no-cost, license-free computing for anyone,

Reducing the cost of education, both for UCF and for our students, is a high priority in the university,

, therefore

BE IT RESOLVED that all IT services that faculty, staff, or students are required to use or that are reasonably necessary for success in their respective roles be based on broadly accepted internet standards. Specifically, for email, these include the Post Office Protocol, version 3 (POP3) or later, and the Internet Message Access Protocol (IMAP). For shared filesystems, this includes the Common Internet File System (CIFS). For printing, this includes the Internet Printing Protocol (IPP).

UCF IT shall promulgate on its web site and by other means the standards, servers, port numbers, and other settings required for self-supporting users of any operating system to connect their computers to campus services.

UCF IT may additionally choose to recommend and support specific client software for specific operating systems, and not to support other software, based on a combination of campus demand and support load and impact.

For users of confidential data, UCF IT may establish restrictions and required training to ensure that such data are not inadvertently disclosed.