IT Security: User Experience Study and Results

Completed by: Doug Horne, Robin Bergart and Juliene McLaughlin

Study Period: January – February 2015

Purpose

At the request of CCS, the Library's User Experience (UX) Team investigated IT security knowledge and awareness on the University of Guelph campus. The following questions, as proposed by CCS, guided the study:

- What do U of G staff, students and faculty know about IT security?
- What strategies do they use to cope with an IT security issue?
- What are common practices with regards to maintaining IT security?

Methods

The UX Team interviewed a total of 16 University of Guelph faculty, staff and students from a variety of departments across campus. The relatively small number of participants afforded us the ability to explore responses in depth and ultimately discover recurring themes and collect valuable insight. See Appendix A for the interview guide.

Student Trends

- Students are conscious and mindful of security on their devices. They take responsibility for security measures that they can control like password protecting their phone and laptops.
    - Several times students mentioned having their social media privacy settings on HIGH.
    - Some students regularly checked the "Recent Scams and Phishing Attempts" webpage to confirm a suspected spam email.
- In general, students do not think to seek out IT support on campus.
    - A common strategy we heard from students who encountered IT issues was to call a relative or friend who was perceived as tech-savvy.
    - Students who had used the IT Help Desk were pleased with the help they received.
    - Students regularly mentioned the importance of anti-viruses in ensuring the safety of their devices. However they were unaware that CCS offers a free anti-virus software, and instead had purchased their own.
- Students are concerned about the safety of their email.
    - Often students are using their Gryph Mail as their "professional" account for career building. One student said, "*Email is a really important method of communication in my life, for job hunting, contacting professors and stuff in a personal and career sense so if that was corrupted in some way that would have a lot of repercussions in my life.*"
    - Students suspect that they could be doing more to protect their email account, but they aren't sure what to do.
- Students expressed interest in learning more about security.

    - A student said, "*I'd be interested to know if there were more security options for me aside from password protected…maybe I should have extra security precautions but I don't know what options are out there."*
    - Another student reiterated, "*I really am interested if some workshops or information sessions come out."*
- All the students we interviewed used cloud storage primarily for school-related work.
- Many students were unaware of the security of the Wi-Fi they were connected to. There was some confusion as to the difference between secure and insecure. The security of Wi-Fi seemed to be less of a concern to students than other features like:
    - speed – the general sentiment is that Wi-Fi is slower now;
    - connection dropping – students complained about getting "*booted off*" more often now with secure Wi-Fi; and
    - re-entering credentials – students are happy that they don't have to re-enter their single sign-on every time they get to campus *"which was really annoying."*

Staff Trends

- Staff regularly rely on CCS support.
    - ALL staff members mentioned that CCS would be their first point of contact if they encountered an IT issue while at work.
    - Staff regularly forwarded phishing and spam emails to CCS.
- Staff are knowledgeable and cautious when interacting with sensitive data.
    - Even staff that did not regularly interact with sensitive data were actively trying to educate themselves about proper procedure in case the need arose.
- Staff are conscious of where they store their work documents.
    - Most staff use the shared drive exclusively to store work-related files because they understand that this is regularly backed up and assume it is more secure than their local desktop.
    - Cloud storage, if used at all, was for personal documents.
- Staff had questions about the difference in terms of security between eduroam and uog-wifi-secure.
    - A staff member said, "*I thought they always had the secure service. My big question is, and I called CCS about this, 'Is eduroam secure? Do I need to worry about anything?' And they said 'no it is the same'. So I'd like to know if that is true."*

Faculty Trends

- In general, faculty put trust in the security of the University's systems and network and assume there are precautions and systems in place to ensure their safety.
    - Faculty do not seem to be overwhelmingly interested in IT security. Perhaps because they assume the University is managing it for them.
- Faculty use an external hard drive to back up their files.

General Comments

- Participants use a variety of devices and regularly mix platforms (often simultaneously).
- Participants were confused about uog-wifi-secure: How is it different from eduroam? What makes it more secure? Why was there a change? Is it different from the "secure" Wi-Fi I was using before?
- Participants assume the University is actively managing IT security for the campus and they trust that these measures (which are unknown to them) are enough.
- Participants are concerned about the safety of their Gryph mail account but, other than regularly changing their password, they are unsure of strategies to protect themselves. (Although they are aware that they should regularly change their password, they do not actually practise this).
- Participants' interaction with CCS ranged from satisfaction to avoidance.
    - In general, students that went to the IT Help Desk were pleased.
    - Unhappiness with CCS mainly stemmed from inefficiency.
- Participants rely on the following techniques to stay safe:
    - Is this website/software/email address reliable and legitimate?
    - Do I recognize it? Many people used Google for more information before downloading new software.
    - Is there a work-around so I can still access the information without opening this email/clicking on this link/downloading this software?
    - Do my family or friends know anything about it?
    - Staff consult their departmental CCS person or CCS website.
- Students use cloud storage primarily for school work. Staff and faculty use cloud storage for personal files, if they use it at all.
    - Some staff and faculty expressed resistance to cloud storage because (1) they did not understand it and (2) they were unsure of how secure it is.
- Because of the different levels of awareness and IT practices across campus, communication about IT security should differ depending on the target audience.

Appendix A

Interview Guide

The Library is gathering information for CCS about how computer security issues play a role in your studies to help CCS improve the computing environment on campus.

1. What computer devices do you use? (Mac/ PC, desktop/laptop/tablet/phone).
2. Have you had any recent experiences where you were concerned about security on any of your devices? How did you address your concerns?
3. In each scenario below, consider:
    - Have you had any experience with this issue and what did you do about?
    - If not, have you heard of this issue? Does it concern you?

    a) You receive an email from an unfamiliar sender and you're not sure if you should open it.
    b) You think someone may be using your email account without your permission.
    c) A website tells you to download special software.
    d) You think your email account is being hacked.
    e) Your computer has a virus.
    f) You think you've received a "phishing" email.
    g) You buy a wireless router and plug it in on campus to connect all your devices.
    h) **STUDENT QUESTION:** Someone is posting malicious information or hacking into someone else's website or email.
    i) **STUDENT QUESTION:** Someone is downloading a lot of music or movies illegally.
    j) **STUDENT QUESTION:** Someone is illegally downloading textbooks for free.
    k) **STAFF QUESTION:** Your department asks you to send a mass email using your personal account.
4. How do you make sure your email account stays safe? Does this concern you?
5. Which social media sites do you use (FB, Twitter, Instagram, etc.). How do you make sure they stay secure? Does this concern you?
6. How do you make sure the files on your computer stay safe? Does this concern you?
    a. Do you back up your files? How?
    b. Do you use cloud storage (e.g. Dropbox, Google Drive)? Why or why not?
    c. **STAFF + FACULTY QUESTION:** Do you ever need to encrypt data?
7. **STAFF + FACULTY QUESTION:** How do you make sure your personal server/student's server is secure?
8. Have you ever used a firewall on your computer? Why?
9. Have you ever needed IT or computer support on campus? Please tell us about that experience. What steps did you take to get help?
10. Have you ever a reported an IT security issue? Please tell us about that experience. What steps did you take to report this issue?
11. Have you ever used the IT Help Desk in the Library? Have you called or emailed CCS for help?
12. Recently campus IT moved to a secure wireless system. Tell us about your experience changing the settings on your devices to the new system.

13. **STAFF QUESTION (IF APPLICABLE):** Are there any special security measures you need to take with the Point-of-Sale terminal where people pay with credit or debit cards?