Welcome to week 2 of National Cyber Security Awareness Month! This week the topic is "Creating a Culture of Cyber Security at Work" and the focus of this article is email, spam, phishing, and malware.

Email is unavoidable in this day and age. Everything from class notes to receipts to the latest information about many topics are all sent via email. Departments email back and forth regularly to coordinate resources, plan meetings, and announce upcoming events. These emails are generally useful, informative or important for any number of reasons and we as users are glad to get them.

The cyber security issue with email is the fact that everyone depends on it to conduct business, share ideas and stay in touch. Malicious parties on the Internet use this dependence to prey on those who either do not understand or are uninformed about the risks of email. There are a number of ways that emails are used for nefarious purposes. The simplest method is to simply send false emails that claim the recipient has won a prize or is the heir of a fortune, or can help someone move money for a percentage of millions of dollars. Often these email lead to malicious websites that ask for personal information or financial information. Sometimes these sites will infect the browser and computer of the unsuspecting visitor who is hoping to cash in on easy money.

Other times, scammers will send emails that claim to be from a bank, or from a legal firm or other form of authority, demanding that the recipient pay a fine or fee, or simply "verify their account". In the first case, payment is almost always "required" in the form of money transfers or other non-standard payment methods. In the second case, the potential victim is asked to send their username and password to confirm that they want to maintain the account. This, of course, should never be done. No legitimate business will ever ask for your credentials via email.

Beyond simple scam emails that are sent out by the millions to anyone and everyone, there is another category of email that is targeted and purposefully sent to either a specific group or to individuals. These "phishing" emails are designed to gain information by impersonating a boss or a teacher, or even (gasp!) an IT department. The emails are labelled as "targeted" because the scammer already knows some information about the organization or person, even if it is just a title, like "CFO", and is trying to exploit what they already know to gain higher privilege or access to information.

The last category of email that is unwanted is malware. Malware takes many forms, from links to malicious sites to infected attachments, including malicious macros. Scammers still send out emails with attachments that have macro viruses in them even though mainstream office products have macros turned off by default. Macros are still used with spreadsheets and documents because of the simplicity of creating them, even twenty years after the first macro virus was sent in 1995. Users should be very suspicious of any document attached to an email, even if the email came from someone they know. It is always best to verify over the phone or in person that the attachment did in fact come from the sender and is legitimate.

It is usually easy to spot simple spam emails. Most have poor grammar, incorrectly spelled words, may include text that is not in the native language of the recipient, and use crazy spellings in the subject to avoid spam filters. More sophisticated spam may look correct, but by hovering over the included links (NOT clicking on them!) the fraudulent web address is revealed. The best weapon of the spam recipient is common sense. If an email claims to be from business ABC, but the links in the email point to XYZ, it is probably not authentic. Targeted phishing attacks are harder to detect, since the scammer may impersonate an authority figure. It is always a good idea to contact the person directly via phone or even face to face, if possible.

Some interesting statistics to finish out this topic. Over the previous thirty days, the college faculty and staff were sent 653,376 emails, 207,632 of which were flagged as spam, and 462 of which were blocked because they contained malware. The students have been sent 712,319 emails, 103,481 of which were flagged as spam, and 96 categorized as malware. This works out to a 49% spam rate for faculty and staff, and a 17% spam rate for students. The lower percentage for students is more than likely because their Berry account is not their primary email account. Both of these spam averages are lower than the general Internet percentage of 62% for the first quarter of 2015.