Report on Phishing

George Mason University
Information Technology Services
Information Technology Security Office

Robert Nakles, Executive Director, SPPM, ITS
Curtis McNay, Director
Karen L. Bates, Communications Coordinator

August 13, 2015

Report on Phishing

Executive Summary

Phishing is one of the most popular ways criminals break into computer systems and gain access to sensitive information and computer networks. By sending an email with a link or by asking for user and password information, criminals are able to gain access to computer networks. In 2014 phishing cost organizations worldwide more than $4 billion a year. When a phishing attempt is successful, it allows criminals to conduct cyberspying, install malware on a computer and gives access to propriety information. It can result in identity theft, interruption of a network and information theft. Experts agree that phishing will not go away and is difficult to control. The way to deal with the dangers of phishing is by providing computer users with awareness about the dangers of phishing and training on how to avoid it.

What is Phishing?

Phishing is when cybercriminals, using a real company's logo or name, trick people into supplying sensitive information such as passwords, usernames, credit card numbers , or bank account information. The criminals use the information for a variety of illegal activities, including stealing money or infiltrating computer networks. When criminals access an organization's computer network, they may spy on the organization, steal additional sensitive information or attack the network with viruses. It is estimated that 23 percent of the recipients of phishing emails open the emails and 11 percent of the people who open them click on the attachments. Of the 23 percent who open the phishing emails, about half of the recipients open the email and click on the link within an hour of the email's arrival.[1]

How does Phishing Happen?

Financial motivation is one of the main reasons behind phishing emails. Phishing emails began during the heyday of America Online (AOL). Criminals would send out emails purporting to be financial institutions and lure people into sending information to steal money from bank accounts. Phishing is the most popular way cyber criminals attack. With more than 200 billion emails sent and received worldwide daily, the opportunities for phishing attacks are plentiful. [2] By spoofing legitimate companies, computer users are tricked into believing the company needs them to urgently reply to a request or some type of adverse action, such as an account suspension, will take place. Unsuspecting computer users often click on links in emails, which have viruses that attack computer networks or take users to a link where the users 'update' their information. The cybercriminals use the information to conduct fraudulent activities. In 2014, phishing attacks cost organizations $4.5 billion worldwide. [3]

Why does it Matter to Mason?

George Mason University is one of the top research universities in Virginia. It has more than 33,000 students over four campuses. It has more than 5,000 employees. That makes Mason a target — an attractive target — for hackers.

---

1 Verizon 2015 Data Breach Investigations Report, Various authors, Verizon Enterprise Solutions, Basking Ridge, NJ

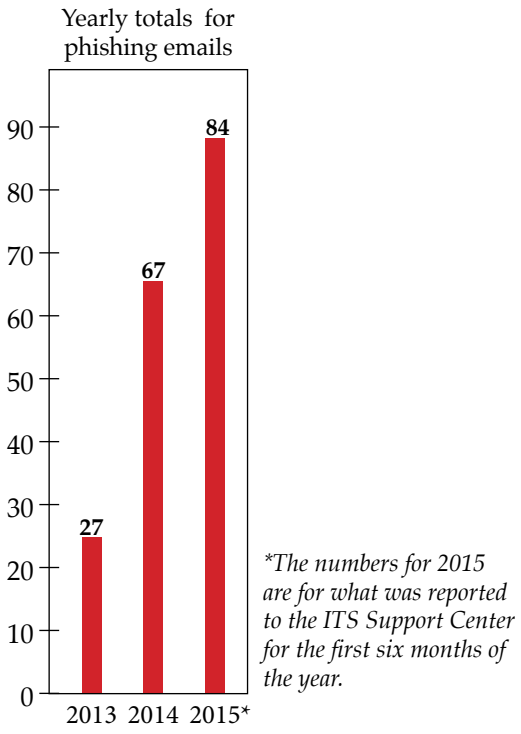
2 Virginia Information Technologies Agency, June 2015 Newsletter Commonwealth of Virginia, Chester, Va.

3 Ibid

In 2013, The New York Times reported that research universities nationwide were facing constant cyberattacks from hackers trying to infiltrate their systems. These advanced persistent threats (APT) call for constant vigilance by the information technology security offices. One university reported more than 90,000 attempts daily to get into its system. The Information Technology Security Office at Mason reported about 20,000 attempts to attack Mason computers during one week in July 2013.

In addition to APT, hackers have become more sophisticated in composing phishing emails, making it more difficult for many computer users to recognize their fraudulent purposes.

Mason has received its share of phishing emails. In 2013, there were 27 phishing emails reported to Information Technology Services Support Center. The number increased to 67 in 2014 and the year-to-date total for 2015 has exceeded the total for 2014 with 84. For 2015 Mason has averaged 14 phishing emails a month.



**The numbers for 2015 are for what was reported to the ITS Support Center for the first six months of the year.*

Cybercriminals are looking for access to information that Mason has. Gaining access to intellectual property, research data, sensitive personal information and the network would give hackers a treasure trove of information.

That is why Internet safety and security is the responsibility of every person at Mason.

Anytime an employee, faculty member, staff member, alumni or student in the Mason network clicks on a suspicious link, that click puts others at risk. When a link is clicked, it can download malware — commonly known as a virus, worm or trojan — on a computer. The malware is used to gain access to the sensitive information of Mason's students, faculty and staff; unleash a program to gain propriety information or provide access to the computer networks to go deeper into network and access affiliated systems; to take down the network and/or to spy.

How Can We Decrease the Risk?

Cyber experts admit that there is only so much that can be done to lock hackers out of computer systems. While there are anti-viruses, patches and security work to keep criminals away, human behavior is one major factor that leaves systems vulnerable.

Every computer user at Mason must be vigilant and make sure he/she is not clicking on links that release viruses or unknowingly providing sensitive information that gives hackers access to their accounts.

Among the ways Mason computer users can protect themselves and fellow Patriots:

- Do not send personal information in an email. No legitimate organization will ask you to do this.
- Keep the operating system, applications and antivirus on computers and mobile devices up-to-date. The updates contain security fixed to possible compromises.
- Do not open suspicious emails or click on links in suspicious emails.
- Report suspicious emails and links. Foward suspicious emails to the Information Technology Support Center by email at support@gmu.edu. Call the Support Center at 703-993-8870 if you need additional help or information.

Appendix

Here are two samples of actual phishing emails sent to Mason community members and ways to tell they are fraudulent.