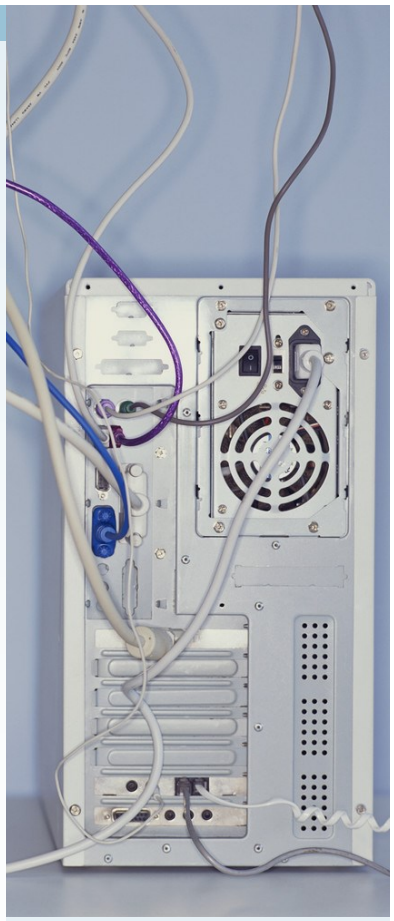
June 2019

LONGWOOD UNIVERSITY

INFORMATION SECURITY



Recent Infection

At the end of May, Longwood was hit by a form of malware known as Trickbot. Malware, short for malicious software, is any software designed to damage, disrupt, harm or compromise any computer, server or network. Viruses, worms, trojans, rootkits, bots, and spyware are all forms of malware.

Trickbot circulated in email that appeared to be from a valid Longwood employee, but was actually from an outside email address. In some cases, the body of the email contained a forwarded email from the reader. The email asked the reader to open an attachment, making the request sound urgent. When the reader opened the attachment and clicked “enable editing” and “enable content,” Trickbot was triggered on the reader’s computer.

Trickbot targets user financial information and drops other malware. If you attempt to do online banking on a computer infected with Trickbot, the malware may obtain your banking information. You can read about it in detail here: https://www.cisecurity.org/white-papers/security-primer-trickbot/.

Fortunately, Information Security and User Support Services were able to contain the incident, and Trickbot only spread to about 45 computers. However, those users lost valuable time as their computers had to be completely wiped of data and “re-imaged.” To prevent the spread of malware in the future, it’s a good idea to be familiar with our policy on malware.

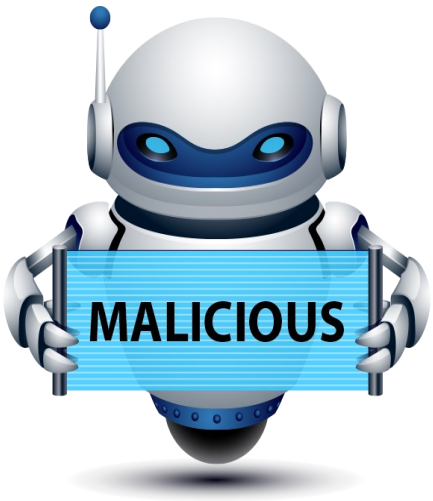
Continued on p. 2

Inside this issue

Special points of interest

- Remember to complete Securing the Human by **10/31/19**.
- Additional access may require additional training; be prepared to finish new modules as they’re assigned.

Recent Infection, Continued



To prevent a malware infection, follow these tips:

Do Not

- Arbitrarily open emails or attachments or click on links
- Respond to emails that request personal information (phishing emails)
- Arbitrarily open files contained on portable media (such as a jump drive)

Do

- Run and maintain malware protection software
- Use operating systems and/or software updates properly
- Validate links, or "hover over" them when navigating the internet
- Compare the name of the sender to the email address
- Validate the email by calling the sender or contacting someone else at the company

Read the full malware policy here.

Did You Know?

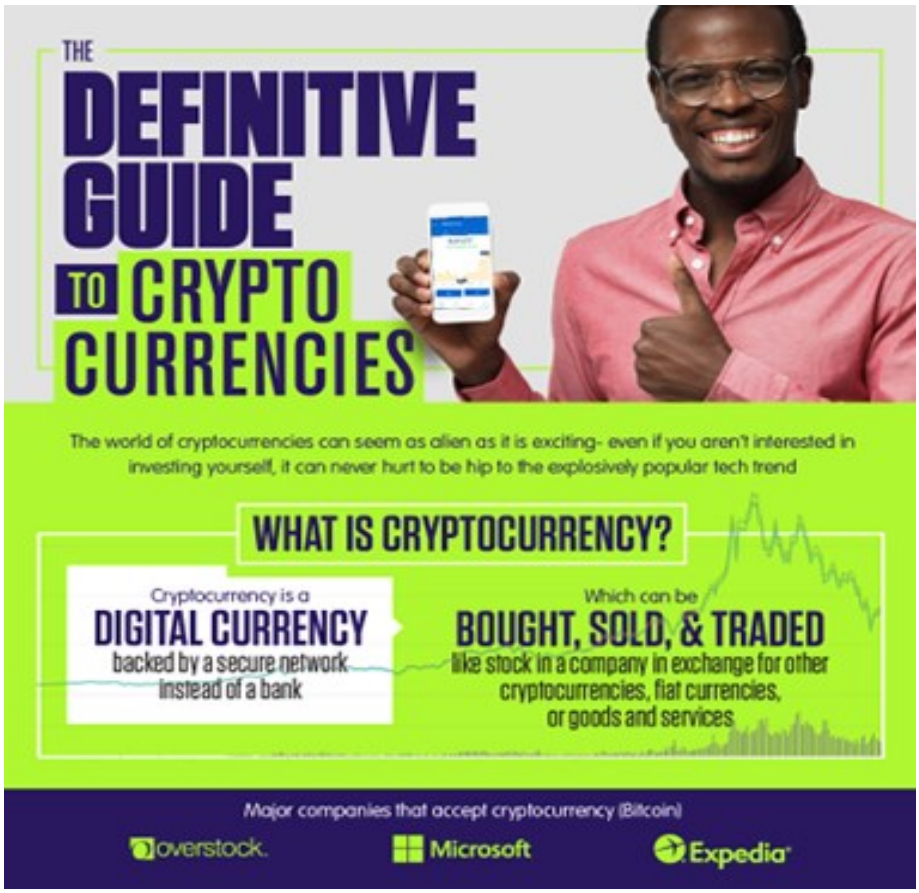
- Malicious bots, like Trickbot, can spread throughout a network quickly.
- Trickbot attempts to disable antivirus programs.
- If your system has been infected with Trickbot, do NOT do online banking on that system. It is best to change your online banking passwords.

About Cryptocurrency

Cryptocurrency comes under many names. You have probably read about some of the most popular types of cryptocurrencies such as Bitcoin, Litecoin, and Ethereum. Cryptocurrencies are increasingly popular alternatives for online payments. Before converting real dollars, euros, pounds, or other traditional currencies into ₿ (the symbol for Bitcoin, the most popular cryptocurrency), you should understand what cryptocurrencies are, what the risks are in using cryptocurrencies, and how to protect your investment.

What is cryptocurrency? A cryptocurrency is a digital currency, which is an alternative form of payment created using encryption algorithms. The use of encryption technologies means that cryptocurrencies function both as a currency and as a virtual accounting system. To use cryptocurrencies, you need a cryptocurrency wallet. These wallets can be software that is a cloud-based service or is stored on your computer or on your mobile device. The wallets are the tool through which you store your encryption keys that confirm your identity and link to your cryptocurrency.

What are the risks to using cryptocurrency? Cryptocurrencies are still relatively new, and the market for these digital currencies is very volatile. Since cryptocurrencies don't need banks or any other third party to regulate them; they tend to be uninsured and are hard to convert into a form of tangible currency (such as US dollars or euros.) In addition, since cryptocurrencies are technology-based intangible assets, they can be hacked like any other intangible technology asset. Finally, since you store your cryptocurrencies in a digital wallet, if you lose your wallet (or access to it or to wallet backups), you have lost your entire cryptocurrency investment.



About Cryptocurrency, Continued

Follow these tips to protect your cryptocurrencies:

- **Look before you leap!** Before investing in a cryptocurrency, be sure you understand how it works, where it can be used, and how to exchange it. Read the webpages for the currency itself (such as Ethereum, Bitcoin or Litecoin) so that you fully understand how it works, and read independent articles on the cryptocurrencies you are considering as well.

- **Use a trustworthy wallet**. It is going to take some research on your part to choose the right wallet for your needs. If you choose to manage your cryptocurrency wallet with a local application on your computer or mobile device, then you will need to protect this wallet at a level consistent with your investment. Just like you wouldn't carry a million dollars around in a paper bag, don't choose an unknown or lesser-known wallet to protect your cryptocurrency. You want to make sure that you use a trustworthy wallet.

- **Have a backup strategy.** Think about what happens if your computer or mobile device (or wherever you store your wallet) is lost or stolen or if you don't otherwise have access to it. Without a backup strategy, you will have no way of getting your cryptocurrency back, and you could lose your investment.

Resources

- Learn more about cryptocurrencies from the FTC article "What to Know About Cryptocurrency."
- Read the *Forbes* article "Guide to Top Cryptocurrency Exchanges" to learn about Bitcoin exchanges and wallets.
- View the A Beginner's Guide to Cryptocurrencies infographic.

The Office of Information Security is responsible for developing and implementing campus-wide policies, controls and procedures to protect the university's information technology resources and systems from intentional or inadvertent modification, disclosure or destruction, as well as monitoring user adherence to these policies.

Tips to Protect Yourself

- Be aware that as a general rule legitimate organizations do not ask for account information in email messages. Know the policies of the organizations with which you do business.
- Never provide your password or other confidential account information in an email.
- Always type in the web address of your bank or any other institution where you have an account and never rely on the links provided in e-mails to access such pages.
- Report phishing messages to phishing@longwood.edu.
- You should never click any links or open any attachments included in phishing messages because of the risk of malware.

Longwood University

Information Technology Services
French Hall
201 High Street
Farmville, VA 23909
(434) 395-4357
(434) 395-2034

Fax: (434) 395-2035