Ransomware?
Have You Heard of It?

MISSISSIPPI STATE UNIVERSITY™
EXTENSION

If it looks real, it must be real, right? Well, this is not necessarily the case when it comes to technology. Email addresses can look so real that it is difficult even to the educated eye to see what is wrong. You most likely get a lot of new emails each day. Many of them you can sort through by just looking in your inbox and recognize them as a phishing email or spam.

What Is Ransomware?

During the holidays, it is easy to lose track of what you've ordered and how items are supposed to be shipped. Often, that is what hackers are hoping will happen, and you can easily fall prey to their "clickbait" trap. Some of the emails delivered to inboxes appear to notify you that a package is being delivered. When you click on the link in the email for the tracking update, your computer becomes infected with ransomware. Ransomware is a type of malware. Specifically, ransomware is a type of malicious software designed to block access to a computer until a sum of money is paid (Rhoades, 2016). There are not many options to block a ransomware attack currently. Ransomware can delete your hard drive completely. It will basically hold your computer files at "electronic gunpoint" (Heater, 2016).

Ransomware comes from Internet connections mostly, but there have been some cases that have involved USB drives. Most cases have been due to the user clicking on a vulnerable link or attachment. Ransomware works quickly, so it will usually infect and possibly encrypt your files before you have time to react.

Ransomware does require you to pay a ransom fee in order to get your files back. They request you use Bitcoins to pay the ransom amount. If your computer is infected with ransomware, you have two options—either pay the amount they ask for or lose your files. If you do not have a backup and you do not intend to pay the ransom, you could lose all your data. So you should ask yourself, "Would it be OK if I lost everything on my computer?" If the answer is no, then you should back up your computer consistently. See MSU Extension Publication 2961 *File Backup Options.*

It is not recommended that you pay the ransom amount because it encourages the criminals to continue attacking. The importance of always maintaining a backup of your files cannot be stressed enough.

How Can I Protect My Device?

The best defense is to not respond or click on any links or emails that you believe are not legitimate. If something appears suspicious, try calling the sender and asking them if they did in fact send you something. Play it safe and check before clicking on an attachment or link. In the event that you do fall victim to an attack, take the following precautions:

- Unplug network or turn off connections to the Internet.
- Hold down the power button until the computer shuts down.
- Unplug the power cord from the computer.

To prevent a ransomware attack:

- Keep your operating system up to date.
- Run malware and anti-virus software.
- Purchase security software.
- Check twice before clicking on suspicious sites, email attachments, or links.

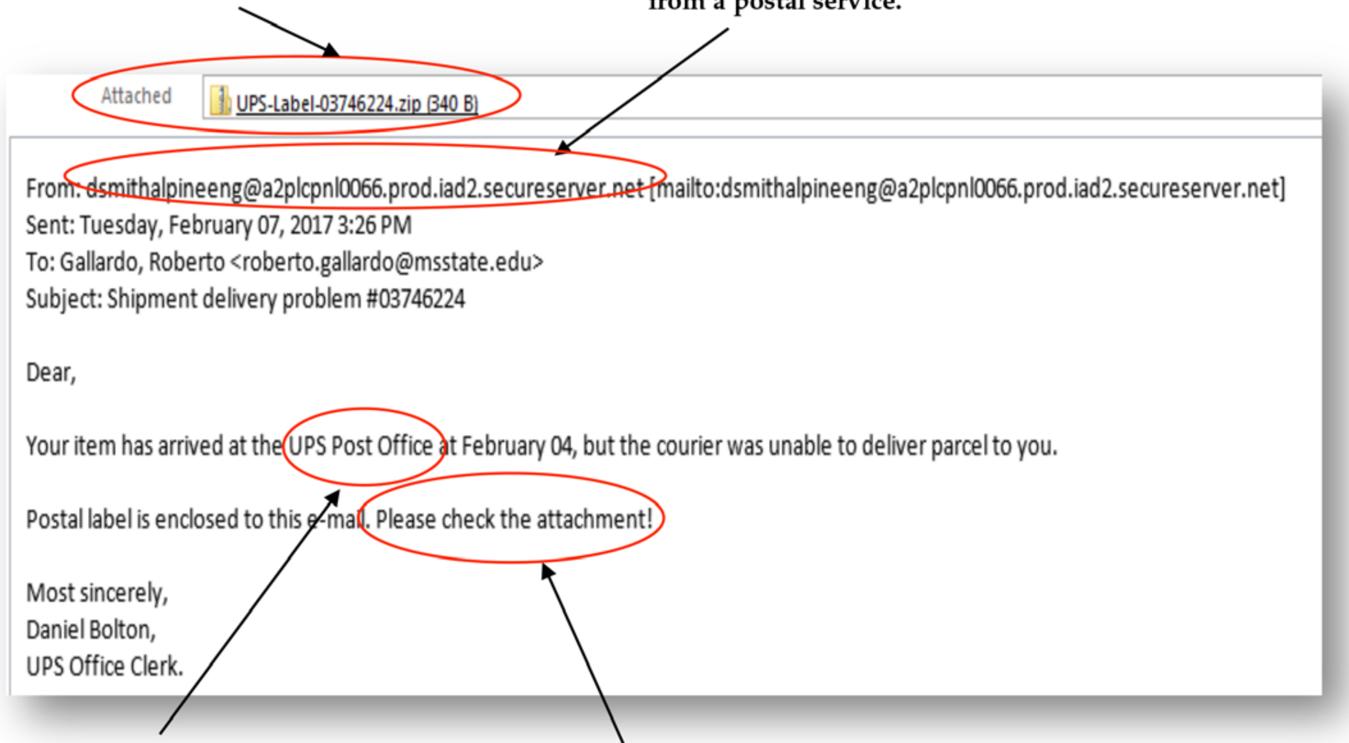
Ransomware is not exclusive to emails; it can also appear as links that you may be tempted to click on through social media sites or even untrusted websites. Once the link is opened, you have started to download the malicious software that encrypts your data. When your files are encrypted, they are converted into another form that cannot be understood by anyone but authorized users.

Bitcoins

Is the word Bitcoins new to you? Well, don't feel left behind. Bitcoin was created in 2009. It is a form of currency that is becoming fairly popular in the Internet world (Zohar, 2015). Bitcoin is an open platform. It is different from a bank in that it is decentralized, whereas a bank is centralized. It isn't owned by anyone, so anyone can use Bitcoins, similar to email. Bitcoins can best be described as digital coins that can be sent through the Internet. Zohar (2015) stated, "Like cash, it is nearly anonymous, and transactions are effectively irreversible once they are committed." In big cities, Bitcoin ATMs can be found. It is fairly simple to gain access to this form of currency. To have a Bitcoin account, you create an account online and link it to a debit or credit card. Bitcoins are kept in your digital wallet, which is a cloud-based service. You can purchase anything with them.

The attachment or "clickbait" contains the ransomware. Do not click on any attachments.

This is not an email address from a postal service.



UPS-Label-03746224.zip (340 B)

From: dsmithalpineeng@a2plcpnl0066.prod.iad2.secureserver.net [mailto:dsmithalpineeng@a2plcpnl0066.prod.iad2.secureserver.net]
Sent: Tuesday, February 07, 2017 3:26 PM
To: Gallardo, Roberto <roberto.gallardo@msstate.edu>
Subject: Shipment delivery problem #03746224

Dear,

Your item has arrived at the UPS Post Office at February 04, but the courier was unable to deliver parcel to you.

Postal label is enclosed to this e-mail. Please check the attachment!

Most sincerely,
Daniel Bolton,
UPS Office Clerk.

If it was from the Post Office, it would be USPS not UPS Post Office.

The sender wants you to click on the attachment that contains the malicious software.

⚠ Make sure the email address does not contain errors.

⚠ An email address should not contain grammatical errors, spelling errors, or a different email address than who the sender is. For example, this email should have been sent from the postal service not the email that it originated from.

Conclusion

Technology users should always be on the lookout for anything that seems suspicious. Being careless with technology can bring about a world of problems that are not only inconvenient, but also costly. “A computer’s security system is only as effective as the person using it” (Heater, 2016).

References

Heater, B. (2016). How ransomware CONQUERED the WORLD. PC Magazine, 109.

Rhoades, G. (2016). Ransomware and other malware. Indexer, 34(3), 126–128.

Zohar, A. (2015). Bitcoin: Under the Hood. Communications of the ACM, 58(9), 104–113. https://doi.org/10.1145/2701411

Publication 3086 (POD-06-17)

By **Jamie Varner**, Extension Instructor, Extension Center for Technology Outreach.

Produced by Agricultural Communications.

Extension Service of Mississippi State University, cooperating with U.S. Department of Agriculture. Published in furtherance of Acts of Congress, May 8 and June 30, 1914. GARY B. JACKSON, Director