Malware/Virus Warning from the Owens GroupWise Email Administrator

Owens Faculty/Staff,

A recent surge in malware threats has occurred at Owens as well as some other area colleges. As you're likely aware from past messages from ITS, there are many forms of email threats. The most prevalent is still the embedded link. But, in the last two weeks, ITS has become aware of a different type of threat in the form of an email attachment. These attachments can be executable files (.exe or .com). The recent threat seems to be in the form of a .zip file attachment (filename.zip). The sender is addressing the email to make it appear to come from an internal Owens employee. The "From:" address may be displayed as: Administrator (voice9@owens.edu). This is not a valid email Owens address. The real address is masked by what's known as a "forged" (or fake) email address, to make it appear that the message is from an Owens email account. The subject of the messages can vary as well.

Opening the attached files can potentially be extremely damaging. Files on your PC and even shared network drives can become damaged, and no longer accessible for all users of shared resources. One specific virus that's been identified recently is what's termed as "ransomware". When the file attachment is opened, it will encrypt files on the local PC as well as attached network drives. It will then pop-up a message on the PC with a ransom demand for a code to decrypt the files. When you check messages in your personal quarantine (MailStore - in Ozone), please be very suspect of any message captured in this quarantine. Messages in MailStore are rated with a SPAM score from 1 - 10, with 10 being the highest threat. Any message with an attachment that is released from MailStore should have the attachment scanned before opening. If your not expecting a message from a sender, or the senders address appears a bit odd or unrecognizable, please contact the HelpDesk at x7120 before opening any attachments or clicking on the email link. It would be a good practice to contact the sender to verify they sent you the message in question if your not sure about it's origin or safety.

Regards,

Dean Niederkohr

GroupWise Email Administrator

Mobile Device Administrator

Owens Community College

Information Technology Services

Owens Faculty/Staff,

Welcome back to a new semester at Owens Community College! Please review the following message regarding SPAM and Phishing email messages that you may receive in your mailbox this school year.

SPAM/Phishing email reminder:

The following are a listing of some of the recent Phishing email messages reported to the Owens Helpdesk. The large majority of these messages are caught by the Owens email firewall. With this system in place, some illicit messages still do get through. SPAM messages can be stopped by adding the sender to your "Block List". All faculty/staff can access their personal email quarantine by logging into Ozone and clicking on the tab named "Mailstore". In this email quarantine, you can review messages that have been tagged as SPAM as well as messages that have been quarantined due to being labeled as having a virus in the message. You also have an option to receive a daily report of activity in the Mailstore by selecting “Preferences” and at the “Quarantine Report Type”, select “Daily Report”. Then click the Save button to confirm the changes. You can access the user guide for the quarantine by cutting and pasting this link into your web browser: (https://intranet.owens.edu/its/mquarantine_userguide.pdf) or by selecting (in Ozone) the "Intranet" tab/Information Technology Services and under Email click on "M+ Quarantine User Guide. This guide will cover the function of your quarantine as well as how to setup "Block Lists" and "Allow Lists".

The most common Phishing message we tend to see still is a request to "Your mailbox is almost full" , "There's a problem with your email account", "Webmail Verification Update" or "Email Quota Limit Exceeded". These messages will likely ask for your Firstname/Lastname as well as your username/password. If you look closely at the sender email address, you will most likely notice that it is NOT an Owens email address that is sending this message to you! Owens ITS would never ask for this information. The other type of Phishing email will ask you click on a link, which will then take you to 3rd party web page. You will then be asked to enter your login/password information for your Owens email account. If you see an email like this, it is referred to as "phishing", or as definition states: The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise/institution in an attempt to scam the user into surrendering private information that will be used for identity theft. If you do receive any messages like this, please forward them as an attachment to the Helpdesk (helpdesk@owens.edu) by Right-clicking on the messages and then selecting to "Forward as an attachment" to the Helpdesk email address. If you do provide your login information in one of these messages, please contact the Helpdesk at (567)661-7120 ASAP so your password can be changed. This will prevent your account from being used to SPAM other individual's email accounts. Viewing the example messages below, you can see there is a wide variety of email's we receive (you may recognize some of them). ITS asks that you be aware of these types of messages, and if you are suspicious, please contact the Helpdesk.

Regards,

Dean Niederkohr

GroupWise Email Administrator

Mobile Device Administrator

Owens Community College

Information Technology Services (ITS)

Article ID: 438

Last updated: 14 Jan, 2014

Revision: 3

Information Technology Services -> Kaspersky Security (Anti-Virus) Software -> Malware/Virus Warning from the Owens GroupWise Email Administrator

http://www2.owens.edu/faq/entry/438/