West Virginia Executive Branch
Privacy Tip

This week's tip is from info@phishlabs.com.

Don't respond to suspicious emails!!

Sometimes when sending phishing emails to clients, a "reply to" address is set up to see if people will reply to suspicious emails…and many do.

Many people interpret the simulations as scams and articulate that in colorful language. Others provide information that would be dangerous in the hands of a threat actor, such as contact information for the appropriate employee to connect with based on the simulation.

While there are some who advocate replying to cyber criminals to waste their time and keep them from exploiting the less aware, responding to suspicious emails is never a good idea for the untrained. It's important to remember that these scammers are in fact criminals and engaging with them is like catching a tiger by the tail.

CNN reported a story where a scammer, using phone calls and emails to try and extort a couple for money, eventually threatened them by describing their house in detail. The threat actor told the couple that he knew their whereabouts and followed with a poignant threat if the didn't pay him what he was asking for.

Outside of threats, here are three reasons why you shouldn't respond to suspicious emails:

1. Future Attacks
Responding to suspicious emails can provide more information about your company, such as how your email signatures look, which can be used in future targeted attacks. We have seen examples of emails that include messages like "How am I doing? Contact my manager at…". All of which provides more data for the cyber criminals to lend credibility to their future attacks.

2. Validating your Email Address
By responding back to spammers, scammers, and cyber criminals alike, you are telling them that your email address is live and active. This makes your email a more valuable commodity for criminals to target or sell to other cyber criminals.

3. Providing your Geo-location

The background information in your emails, known as headers, contains information about your location. This can be combined with publicly available information to narrow down your location and find you in the world. In light of the story above, giving up your location to cyber criminals, intentionally or unintentionally, is never a good idea.

While it could be a lot of fun to mess with criminals, it is a dangerous business. When you receive a suspicious email in the office, report it to the appropriate IT or security team[1] and let them handle it. In your personal email account, it is best just to delete them and move on with life. Handling suspicious emails this way further protects you and/or organization from cyber criminals.

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.

[1] Contact WV Office of Technology. 304-558-9966, 1-877-558-9966, or forward email to otphishing@wv.gov