

West Virginia Executive Branch Privacy Tip



PHISHING SCAMS

"Phishing" continues to be one of the biggest threats to online privacy & security. It occurs when a criminal tries to trick you into visiting a malicious website or providing personally identifiable information (PII) which can be misused. Sometimes the phishing attack wants sensitive PII, such as a Social Security Number, but often times the thieves just want to capture your username and password so they can access your computer themselves. Sometimes data thieves steal email addresses, such as an office directory or "contacts" list, in order to target their phishing attacks. This is known as "spear phishing."

Some phishing emails appear to come from reputable companies (such as financial institutions, credit card companies or employee benefits providers) but they actually come from thieves! These emails may indicate that there is some problem with your account. For example, the message may say that they have detected a fraudulent transaction. The email asks you to login to your account to address the issue. However, when you follow the link in the email to login, you are directed to a fraudulent website. If you enter PII, you are providing it to the criminals.

- Be suspicious of all email messages, even if the messages appear to be from a company you trust or a person you know. Verify that the email is legitimate by contacting the company or the person using an email address or phone number that you know to be valid. Do not respond to any email requests or follow any links until the sender's identity has been verified.
- Never open an unexpected attachment – even from someone you trust – if you have not scanned that attachment for virus and malicious code. Even friends may inadvertently send you malicious attachments.
- If you have "clicked" on an attachment – contact your designated Security Representative IMMEDIATELY!

The WV Office of Technology has provided the following information for those agencies on the "wv.gov" domain:

If you receive a suspicious email, DO NOT open the attachment. Simply delete the email and contact the Service Desk (304-558-9966 or Toll Free 877-558-9966).

If you opened the attachment, immediately do the following:

- Turn off the computer
- If applicable disconnect the network cable from the computer
- Contact the Service Desk to report the issue
- DO NOT turn the computer back on until a technician has checked the computer or instructed you to do so

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