WV Executive Branch Privacy Tip
March 2023
Don’t Click the Bait!!
(WHEN IN DOUBT, FORWARD TO OTPHISHING@WV.GOV)

The most common technique that hackers and identity thieves use to compromise accounts and install malware is phishing (pronounced fishing). Why is this? Quite simply, it is effective. These scammers want users to either reply with information, open attachments, or follow a link. The tactics are becoming much more sophisticated and convincing – using common business words like “invoice,” “reports,” or “late fees.” That makes it very important for users to be diligent, even when opening emails from co-workers or friends. THINK BEFORE CLICKING!

1. FROM:

Do you know the person or agency that is emailing you? Were you expecting an email from them? Does it make any sense for that person or that agency to be contacting you? If an unexpected email arrives from an unknown individual, do NOT click on any links in the email or open any attachments.

2. TO:

Is the email directly to you? Was it sent to a random group of people? If the “To” field is empty, it means the sender is hiding that information. While this is a legitimate tactic when sending emails to large groups (ex. newsletters), scammers use it so you can’t see how many people are getting the same email.

3. SUBJECT LINE:

Is the subject relevant to you? Is it relevant to your agency? Most phishing emails will have a short subject line that catches your attention, while providing no specific information. If the subject line or message body before the attachment seems unusually vague, incoherent, or incomplete, delete the email.

4. ATTACHMENTS:

Does the attachment have a random name or have a random number? Does the attachment seem relevant? Were you expecting an attachment from that agency or person? Never open unexpected attachments. Assume an attachment is hostile. If you do know the person in question, but weren't expecting them to send you an attachment, contact them and confirm that they sent it before you open it. If you do know the person in question, but weren't expecting them to send you an attachment, contact them and confirm that they sent it before you open it.

5. MESSAGE:

Does the message text have grammatical errors? Does it threaten to close or limit your accounts? Or, does it provide no information at all? Be suspicious of any email that requires immediate action or creates a sense of urgency. Be suspicious of grammar or spelling mistakes, most people proofread their messages very carefully. This is a common method used to trick people. If a link in an email seems suspicious, hover your mouse over the link WITHOUT clicking. This will show you the true destination -- where you would go if you actually clicked it. The link that is written in the email may be very different from where it will actually send you.

If you receive a suspicious email, forward it to otphishing@wv.gov. If you've clicked on a link or opened a document from a phishing email, please contact the Service Desk immediately so the appropriate remediation can be taken.

Also, please note: don't send the email (with link or attachment that is causing the suspicion) to your supervisor, your HR person, your privacy officer or to the State Privacy Office, send it directly to otphishing@wv.gov. Sharing the email with the suspicious components only heightens the risk that someone will accidentally click it.