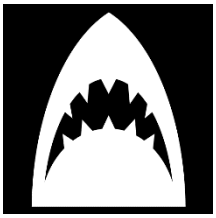
West Virginia Executive Branch
Privacy Tip

Do You Know Your Phish?



Phishing emails are messages that look legitimate, but they have malicious intent. Most of us have had training on how *not* to take the bait, but studies show that 90% of employees would click on a phishing email within an hour after the training!

According to the 2019 Verizon Data Breach Investigations Report (DBIR), phishing is the #5 cause of security incidents, however it is the **#1 cause of data breaches**. The security incidents can also involve phishing, by way of malware or stolen credentials. Over 94% of malware is delivered through phishing emails.

So, do you know your phish?

- Phishing emails & text messages usually look like they are from a legitimate source.
- They will claim there is suspicious activity or log-in attempts on your account.
- Asks you to click a link to confirm your account name/number and password.

Phishing emails to your work account may look a little different.

- A phisher will spoof a legitimate email address from another employee or boss.
- They may ask you to send personal information (such as employee W-2 forms) to them.
- Or they may send an urgent email that has an attachment that must be opened ASAP.

So – what do you do?

- If it is a business asking for information, call them using a phone number on their actual web page, not one in the email.
- If it's a work email – call the individual to confirm they sent the request.

And always –
If you encounter a suspicious email, please forward it to OTPhishing@wv.gov or ServiceDesk@wv.gov. If you have fallen victim to a phishing attempt or you believe your account or computer was compromised, please contact the Service Desk immediately at the above email addresses (from another computer) or by calling 304-558-9966 or Toll Free 877-558-9966.

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