JULY PRIVACY TIP

WV State Privacy Office

PHISHING

- IS A FORM OF SOCIAL ENGINEERING; CYBERCRIMINALS USE EMAILS, SOCIAL MEDIA, OR MALICIOUS WEBSITES TO POSE AS A TRUSTWORTHY ORGANIZATION OR PERSON AND SOLICIT PERSONAL INFORMATION.

Every day phishing emails are sent to inboxes. While some of these are obvious frauds, others can look legitimate. How can you tell the difference? Here are some things to look for.

1. **Check the email address in the header – if it looks suspicious, don't open the email**

Sometimes the "from" address in a phishing message will appear to be perfectly valid. However, if the email has a "@business.business" different from the company name that is displayed, the message is probably fraudulent or malicious.

2. **Look, but do NOT click**

Hover your mouse over any links embedded in the body of the email. If the link address looks weird, don't click on it. If you want to test the link, open a new window and type in website address directly rather than clicking on the link from unsolicited emails.

3. **The message contains poor spelling and grammar – but not always!**

Whenever a large company sends out a message on behalf of the company, the message is usually reviewed for spelling, grammar, and legality, among other things. If a message is filled with poor grammar or spelling mistakes, it probably didn't come from a major corporation. But scammers are getting smart, so be careful!

4. **The message asks for personal information**

A reputable company will never send an email asking for your password, credit card number, or the answer to a security question. When in doubt, call the business using a phone number on a statement or their official website, not one in the email.

5. **The email has urgent language**

Beware of messages that suggest your account has been suspended, or there's been some suspicious activity. A sense of urgency is a common tactic in phishing. Once again, do not give any personal information and call the business directly.

6. **The email is from a government agency**

Also, beware of messages claiming to have come from a law enforcement agency, the IRS, the FBI, or another entity that might scare the average law-abiding citizen. The US Government agencies do not normally use email as an initial point of contact.

If you encounter a suspicious email, please forward it to *OT.Phishing@wv.gov* or *ServiceDesk@wv.gov*. If you have fallen victim to a phishing attempt or you believe your account or computer has been compromised, please contact the Service Desk immediately at the above email addresses or by calling 304-558-9966 or Toll Free 877-558-9966.