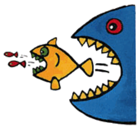
West Virginia Executive Branch
Privacy Tip

PHISHING IN THE NEWS



The IRS has reported that hacker attacks using phishing and malware have surged **400%** this tax season alone. Sometimes a hacker manages to send the right fake email to the right person, and they get everything they want. Major tech company Snapchat found that out the hard way.

According to the Official Snapchat blog, “Snapchat’s payroll department was targeted by an isolated email phishing scam in which a scammer impersonated our Chief Executive Officer [Evan Spiegel] and asked for employee payroll information. Unfortunately, the phishing email wasn’t recognized for what it was–a scam–and payroll information about some current and former employees was disclosed externally.”

This is a good reminder that anyone can fall for a phishing email if it comes from the right source or says the right thing. It takes just one mistake for your information to end up in the hands of hackers; and it doesn't even have to be your mistake. What to look for in a phishing email:

- **Generic greeting.** Phishing emails are usually sent in large batches. To save time, Internet criminals use generic names like "Bank Customer" so they don't have to type all recipients' names out and send emails one-by-one. If you don't see your name, be suspicious.
- **Hyperlinks.** Even if a link has a name you recognize somewhere in it, it doesn't mean it links to the real organization. Roll your mouse over the link and see if it matches what appears in the email. If there is a discrepancy, don't click on the link. To be safe, don’t use a hyperlink at all – type the correct web address in the address bar of your computer. You can verify the validity of the email request by contacting the organization directly.
- **Requests personal information.** The point of sending phishing email is to trick you into providing your personal information. If you receive an email requesting your personal information, it is probably a phishing attempt. Again – contact the organization directly to be certain you’re giving your information to the legitimate organization.
- **Sense of urgency.** Internet criminals want you to provide your personal information now. They do this by making you think something has happened that requires you to act fast. The faster they get your information, the faster they can move on to another victim.

23% of recipients open phishing messages. 11% click on attachments. Numbers show that with just 10 emails, there is a greater than 90% chance that at least one person will be hacked. 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.

If you encounter a suspicious email, please forward it to OT.Phishing@wv.gov or ServiceDesk@wv.gov. If you 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 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.