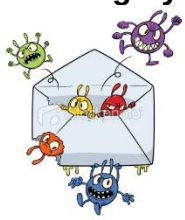
West Virginia Executive Branch
Privacy Tip

Email Bugs & Naughty Hyperlinks



Recently, we sent a tip dealing with “phishing” emails. One of the biggest dangers of these emails is accidentally introducing a virus into the system. Unfortunately, 11% of recipients of phishing emails click on attachments or links within the email. Numbers show that with just 10 emails, there is a greater than 90% chance that at least one person will be hacked.

Most viruses spread by emails come one of two ways - in an attachment, or through a link to an infected website. Either way, you have to click on it to activate it. So don't! Almost all the email attachments we care about we are expecting or know what it is. You do not have to open every email you get, and you do not have to look at every attachment.

In 2009, a poisoned email that looked like it came from Fed Ex contained a nasty virus. The email said the attachment had order details in it. Recipients didn’t recognize what the Fed Ex email was talking about, so of course they clicked on the “Order Details” attachment to find out more...and that’s when the virus was activated. Moral of the story: If you receive e-mail attachments that you aren't expecting, you should contact the sender directly to verify they sent it before you open anything.

Hyperlinks within an email can also be used to transmit viruses. Some use a legitimate website's look but redirect to another bogus website or pop-up window. This is where malicious software can be downloaded onto your computer. Do not click a link in a message, without first rolling your mouse over it. This will usually show the address where the link will take you. The safest way to confirm if a link is valid is to type the proper web site address in your browser.

Remember – don’t just blindly click on links or open attachments without first verifying their validity!

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 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.