

alpha  
TECHNOLOGIES




ONE CALL, ONE COMPANY, FOR IT PEACE OF MIND.

# OCTOBER IS CYBER SECURITY AWARENESS MONTH



## Week 3: Phishing

Alpha Technologies, a leader in technological innovation, takes this opportunity to promote cyber hygiene, raise awareness about online risks, and share insights and best practices for maintaining robust digital security.



Phishing attacks have become increasingly sophisticated and prevalent. These online scams can lead to severe consequences, including identity theft, financial loss, and compromised personal information. However, with a keen eye and the right knowledge, you can learn how to spot phishing attempts and protect yourself from falling victim to these malicious schemes. In this week's newsletter, we'll guide you through the key signs to watch out for when identifying phishing attempts.

### **Check the Sender's Email Address**

The first and most crucial step in identifying a phishing email is to scrutinize the sender's email address. Cybercriminals often use deceptive email addresses that appear legitimate at first glance. Look closely for subtle variations or misspelled domain names. For instance, if you receive an email from "service@paypal.com" that looks suspicious, it may come from "service@paypall.com." Always verify the sender's address before taking any further action.

### **Sense of Urgency: Beware of Urgent Language**

Phishing emails often employ urgent language to create a sense of panic and pressure you into taking immediate action. Watch out for phrases like "your account will be suspended," "urgent security alert," or "immediate action required." Legitimate organizations usually communicate important matters professionally and calmly, without pressuring you to make hasty decisions.

### **Look for Spelling and Grammar Errors**

Many phishing emails originate from non-native English speakers, which often results in noticeable spelling and grammar mistakes. Keep an eye out for poorly constructed sentences, awkward language, or unusual word choices. These errors can be indicative of a phishing attempt. As AI is leveraged to create phishing messages, spelling and grammar errors are going to be less frequent.

### **Verify Links and URLs**

Hover your mouse cursor over any links or URLs provided in the email without clicking them. This action will reveal the actual web address you will be directed to. Phishers often mask malicious websites with genuine-looking links. Ensure that the URL matches the official website of the organization or service it claims to represent.

### **Check for Unsolicited Attachments**

Be cautious when encountering unsolicited email attachments, especially if you weren't expecting to receive them. Cybercriminals often use attachments to deliver malware or viruses to your device. Never open an attachment from an unknown source, and always verify its legitimacy with the sender before taking any action.

### **How To Respond**

In your business, if you have a mechanism to report suspected phishing email, report it. Reporting will let the security team analyze the message and disable any call to action for the entire organization, which helps to protect the organization against future attacks.

Phishing attacks continue to evolve and adapt, making it crucial for individuals to stay vigilant and informed. By following the steps outlined in this article and practicing good cybersecurity hygiene, you can significantly reduce your vulnerability to phishing attempts. Always remember that it's better to be cautious and double-check suspicious emails than to fall prey to a cybercriminal's tricks. Your digital identity and security are worth the extra effort to stay safe online.



Tony Schliesser – Chief Information Security Officer Alpha Technologies.

Hurricane WV • 304-201-7485 • [www.alpha-tech.us](http://www.alpha-tech.us)

