AppState InfoSecurity Bits & Bytes

January 2017

A monthly newsletter brought to you by the Office of Information Security

Stay Connected!

Follow us **@appinfosec**

Like us **Facebook.com/appstateois**

Email us: **security@appstate.edu**

Visit us: **security.appstate.edu**

Information Technology Services
APPALACHIAN STATE UNIVERSITY

Information Security
App State

AppState Cybersecurity Report

ITS has observed several sophisticated phishing attempts recently.

Here are a few tips that can help:

- Always check the "From" field of the email to validate that the message actually originated from the correct AppState account. Remember that the name of the sender in email can easily be forged.
- Look for attachments or images that may be used as substitutes for the text body of the messages or contain an embedded link. Never click on an attachment or link in a suspect message.
- If you believe you have been a victim of a phishing attempt, please contact the ITS HelpDesk for immediate assistance at (828) 262-6266.

Need to report a suspicious email?
Email us at:
phish@appstate.edu

Guard Your Privacy Online

You and your information are everywhere. When you're online you leave a trail of "digital exhaust" in the form of cookies, GPS data, social network posts, and email exchanges, among others. It is critical to learn how to protect yourself and guard your privacy. Your identity and even your bank account could be at risk!

Helpful Tip

Use long, complex #passwords or #passphrases as your first line of defense to protect online accounts. #Privacy

TIPS FOR PROTECTING YOUR ONLINE PRIVACY:

USE LONG & COMPLEX PASSWORDS OR PASSPHRASES	These are often the first line of defense in protecting an online account. The length & complexity of your passwords can provide an extra level of protection for your personal information.
TAKE CARE WHAT YOU SHARE	Periodically check the privacy settings for your social networking apps to ensure that they are set to share only what you want, with whom you intend. Be very careful about putting personal information online. What goes on the internet—usually stays on the internet.
GO STEALTH WHEN BROWSING	Your browser can store quite a bit of information about your online activities, including cookies, cached pages, and history. To ensure the privacy of persona information online, limit access by going "incognito" and using the browser's private mode.
USING WI-FI?	If only public Wi-Fi is available, restrict your activity to simple searches (no banking!) or use a VPN (virtual private network). The latter provides an encrypted tunnel between you and the sites you visit.
SHOULD YOU TRUST THAT APP?	Only use apps from reputable sources. Check out reviews from users or other trusted sources before downloading anything that is unfamiliar.

James Webb, *Chief Information Security Officer*

Oscar Knight, *Policy & Compliance Coordinator*

Appalachian STATE UNIVERSITY Office of Information Security

Kevin Wilcox, *Security Operations Coordinator*

Crystal Brooks, *Security Awareness Coordinator*