Security Awareness Training

- **Be aware of online scams** - don't get lured by phishing! Report any attempts to get your username, password, or other personal information to phish@appstate.edu. Don't share your password, and never enter your password on a website without making sure you are in the right place. Appalachian ITS will never ask for your password!
- **Use Good Passwords and Keep them Safe:** Use passwords with letters, numbers, and symbols - for each account. If you need help remembering your passwords, use a password vault like KeePass.

- **Review your Social Media Privacy settings** - customize your privacy settings and think about what you share.
- **Don't link your social media accounts together** - one hacked account gives the hacker access to all linked accounts.
- **Be aware of online scams** - don't get lured by phishing!
- **Log Out before you walk away from a public computer** - log out of your Google account and the public computer.
- **Keep clean machines and back up your files** - Make sure your device and software are set to install regular updates and use Antivirus software. Back up your files with an external device and/or Google Drive.
- **Use https** - whenever you transmit confidential information to a website.
- **Be careful where you click:**
    - Use official sites like Google Play Store to download apps, and review what they want to access.
    - Don't open questionable email attachments or click on ads on websites.

In addition to the security tips outlined above, Faculty and Staff:

- Keep your office computer on 1 night during the week to get IT updates.
- Lock your computer when you step away.
- Know our Guidelines for Storing & Sharing University Information
- **Use uDesk --** a remote virtual Windows desktop that runs on your computer -- when appropriate. If you visit a site with malware in uDesk, your computer won't be infected.
- **Back up your files to uStor P: drive.**
- **Use a secure wireless connection** - Use "asu" secure wireless network, or use ASU VPN when you connect to public wireless.

Additional Self-Training Information

What is Phishing?
"Phishing" refers to the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. These attempts by cybercriminals, nation states, or hacktivists to lure you into giving away personal information, to gain access to accounts, or to infect your machine with malware & viruses are a form of social engineering. Like all universities, Appalachian State University is frequently phished for account credentials. Phishing attempts can happen through a variety of channels, including email, social media, or text messages, and can compromise security and lead to the theft of personal and financial data. Highly targeted attacks on groups or individuals are known as “spear phishing.”

What tactics are used in phishing attempts?
Phishing messages can come from hijacked accounts of people you know, making them hard to distinguish from real messages. Additionally, cybercriminals commonly use infected documents or PDF attachments as vectors for their phishing attempts. Another common trick attackers use is trying to get victims to sign in on a fake login page where their usernames and passwords can be stolen.

How do you avoid phishing attempts?
Phishing attempts can often get through spam filters and security software that you may already have in place, so stay vigilant and trust your instincts. Keep an eye out for things like unexpected urgency or a wrong salutation. Think twice about clicking a link or opening a document that seems suspicious. Double-check that every URL where you enter your password looks legitimate. And if anything raises doubt, report the communication to phish@appstate.edu.

As part of our ongoing efforts to help defend App State from increasing cybersecurity threats, ITS will be sending out test phishing emails. **These internal phishing messages are learning opportunities and employees will not be punished for falling victim to a test phishing attack.**

These test phishing messages will simulate real-world attacks that are often observed in our security monitoring practices. These test messages will be sent out at random intervals throughout the year.

Key Takeaways:

- Phishing test messages will simulate real-world phishing attempts, starting with easily identifiable phishing scenarios and progressing to more advanced scenarios as employees improve their responses.
- Employees who receive suspicious emails should forward them to phish@appstate.edu, regardless of if they think it is part of the test or not.
- **The results of these phishing tests are only visible to the ITS Office of Information Security**.
- Reporting on these tests will be anonymous.
- If you click on a link in one of these messages, you will receive information to help spot and avoid similar phishing messages in the future. Employees who fall for a phishing attempt will be redirected to an educational webpage comprised of phishing information and training opportunities, including the identification of specific elements within the message that would help to distinguish it as fraudulent.
- ***Our goal is to increase employee security awareness and decrease the number of employees who click on malicious emails.***

With all suspicious emails, remember these helpful steps:

1. Look at the sender's email - is it an App State email? Is this someone you know?
2. Are they asking for personal information? Or for you to download an attachment?
3. Don't click on links if the email seems suspicious or unusual.
4. You can help us to identify suspicious emails by forwarding them to phish@appstate.edu.

A Few Important Things to Remember

- Always remember that ITS will **never** ask you to provide your password either via the phone, email, or other communications.
- Keep in mind that phishing emails can look very legitimate and include the same images, logos, and text associated with the organizations they are attempting to masquerade as. Don't take the appearance of an email or website as a mark of legitimacy.
- Be aware that the 'From' field in email messages can easily be fabricated. Don't assume that an email is legitimate based on the apparent sender in the "From" field.

Employees are strongly encouraged to treat all suspicious emails as potentially dangerous. While these simulated messages are not malicious, real phishing attacks pose a great threat to our university community.

Addition Resources

Phishing Examples:

Common Security Threats

Videos:

- http://www.antiphishing.org
- https://www.us-cert.gov/ncas/tips/ST04-014

Online Quizzes:

- http://www.sonicwall.com/furl/phishing/
- https://www.paypal.com/webapps/mpp/security/antiphishing-canyouspotphishing

Protect your valuable work, music, photos & other digital information by making an electronic copy & storing it safely. If you have a copy of your data and your device falls victim to ransomware or other cyber threats, you will be able to restore the data from a backup.

Back up your data regularly, and make sure your anti-virus software is always up to date. Several options are available for backing up your data, including:

- Back-Up To an External Drive
- Back-Up Over the Internet
- Use a Cloud Storage Service

Be conscientious of what you plug into your computer. Malware can be spread through infected flash drives, external hard drives, and even smartphones. Always be careful when clicking on attachments or links in emails. If it's unexpected or suspicious for any reason, don't click on it. Double-check the URL of the website the link takes you to bad actors who will often take advantage of spelling mistakes to direct you to a harmful domain. When in doubt, forward the message to phish@appstate.edu.
Keep all software on internet-connected devices (including personal computers, smartphones & tablets) current to reduce the risk of infection from ransomware and malware.

Why is updated software important?
Running out-of-date software can put you at risk of security vulnerabilities that hackers seek out & exploit. Security experts agree that keeping your software - including Internet browsers, operating systems, plugins & document editors - up-to-date on internet-connected devices is fundamental cybersecurity practice & helps prevent malware infections that could compromise your devices & accounts.

Why is preventing malware important?
Malware can take many forms, including capturing keystrokes and passwords when they are entered, ransomware, which can encrypt files and demand payment to release them, and using devices to send out spam or participate in a distributed denial of service (DDoS) attack. If your device is infected, sharing files may also infect others.

How do you keep software up to date?
When you receive a notification that a software update is available, install it as soon as possible. Knowing your programs and operating system is important. Some programs, like reputable antivirus/security software and some web browsers, including Chrome, automatically update. Mobile operating systems, apps, and other critical software may require your action to update.
Be sure to monitor your accounts, both financial and social, for any suspicious activity. If you see something unfamiliar, it could be a sign that you've been compromised.
Never leave your devices unattended. If you need to leave your computer, phone, or tablet for any length of time (no matter how short) lock it up so no one can use it while you're gone.
Information about you, such as purchase history or location, has value (just like money). Be thoughtful about who gets that information and how it is collected by apps, websites, and all connected devices. Set the privacy and security settings on websites to your comfort level for information sharing. It is OK to limit how and with whom you share information.

Share With Care
Think before posting about yourself and others online. Consider what a post reveals, who might see it, and how it might affect you and others.
Practice good password management. Use a strong mix of characters, and don't use the same password for multiple sites. Don't share your password with others, don't write it down, and definitely don't write it on a post-it note attached to your monitor.
Why should you secure your mobile devices?
Mobile phones & tablets contain a wealth of personal data, including emails, contacts, schedules, locations, and direct access to apps. When your mobile device is lost or stolen, your data goes with it, making any information contained on the device vulnerable.

How do you secure your mobile devices?
The first layer of mobile security is locking your device with a passcode, Touch ID features, or other biometrics. In case your phone is ever lost or stolen, make sure you're aware of the different offerings that exist to help you remotely locate or lock your device, or wipe data from it. Some of these features may be built in by the operating system or carrier (They may albo be available via an app.) Your systems administrator might also have specific rules to follow if you lose a work device.
Sensitive browsing, such as banking or shopping, should only be done on a device that belongs to you, on a network that you trust. Whether it's a friend's phone, a public computer, or a café's free WiFi, your data could be copied or stolen.
Why use security tools?
Many online service providers offer useful settings and tools to help you manage your online presence, keep your data secure, and get the most out of the services you use. For example, strong authentication is rarely turned on by default but is offered by many online services for users that want an extra layer of protection on their account.

How do security checkups work?
Guided security checkups help you understand the security settings available, and give you confidence that you are using the strongest options available. And managing your notification settings, including alerts when your location is being used or when new information about you or a new photo is posted online, can help you manage your online presence.
Why are unique passwords important?
Password reuse for multiple accounts is one of the most common ways accounts are hijacked. When passwords are reused, having your credentials stolen for one account means hackers gain access to other accounts that use the same login details.

What makes for a strong password?
In addition to being unique, security experts agree that a strong password is at least 12 characters long, and contains a mix of letters, numbers, and symbols. Maintaining strong and unique passwords will decrease the risk of password guessing based on commonly used passwords, information about you that might be publicly available, or password-cracking tools that hackers use.

How do you manage better and unique passwords?
It is really hard to remember a lot of strong and unique passwords. Thankfully, there are a lot of tools out there to help. Using a password manager only requires you to remember one master password to access your other passwords. If needed, you can write passwords down on a piece of paper and store them in a secure location away from your computer, but be careful not to store passwords right on your computer.
Realize that you are an attractive target to hackers. Don't ever say, "It won't happen to me." You may not realize it, but you are a target for cybercriminals. Your computer, your mobile devices, your accounts, and your information all have tremendous value to cybercriminals around the world.
For policies, standards, guidelines & tips see our security.appstate.edu
To get help with your personal devices at our Technology Support Center
You can enter a support ticket at support.appstate.edu
If you have any information security concerns or questions you can email support@appstate.edu, contact your ITS Consultant, call the ITS Support Help Desk at (828) 262-6266, or visit the Technology Support Center in Room 140 of Anne Belk Hall (Exterior entrance located directly across from Rankin Science)

Related Articles

- AnyConnect VPN Articles
- Cannot log into Computer after password change.
- Common Security Threats
- Connect to ASU network using AnyConnect VPN
- How to Update my Appstate Password
- Mobile Device Security Guidelines
- Remote Connection
- Security
- Security and Google Apps
- Security Awareness
- Security Awareness Tools and Resources
- uDesk Virtual Desktop Articles
- Unlocking Bitlocker-Locked Computer
- Work from Home (Telework) Resources

We value your feedback! Click HERE to suggest updates to an existing article, request a new article, or submit an idea.

Search Knowledge Base

Submit a Service Request