Cybercrime Prevention Tips

Ways to Protect Yourself

In today's society, cybercrime is one of the fastest growing criminal activities. A recent study has found that one in every five Americans has had an account compromised or personal information stolen. Aside from financial fraud or on-line identity theft, other types of cybercrimes include, bullying, email spoofing, stalking, hacking, information piracy and forgery, as well as intellectual property crime.

Here are a number of ways to better protect yourself against computer crime.

- **Lock or log off your computer when you step away**. You want to make sure no one else has access to all your information.
- **Use security settings**. Use PIN's or passcodes to protect yourself from someone accessing your information. Use Multi-Factor authentication (Like SU'S DUO service) wherever possible, this will cut down on the ability for your identity to be compromised significantly. Do not reuse passwords and a password manager to store/generate passwords. If you suspect your accounts have been compromised change your password(s).
- **Have current security software and update it regularly**. The latest security software protects against viruses, malware and other on-line threats.
- **Consider sharing less online**. The types of information you should avoid sharing include your date of birth, geographic information, and personal family information such as pet names or the city you live in. Do not share when you are going on vacation, but maybe share when you get back. Social media profiles give criminals a more complete picture for them to steal your identity.
- **Verify Email Senders**. If an email looks suspicious, asks for personal information, or appears from a superior asking you to perform a favor always verify the sender. For email to your University account, any email sent from a non-University account will have a banner at the top informing you that the email originated from outside the University.
- **If it looks suspicious, don't click**. Your information can be compromised by cyber criminals through, posts, tweets, emails and online advertising.

If you are in doubt, just delete it. Beware of anyone who requests that you act immediately.

- **Be careful using public Wi-Fi**. Public/Unencrypted Wi-Fi is easily connected to by Hackers. Every move you make can be watched including what passwords and account information you enter while connected.

* The Salisbury University Police Department would like to thank the Salisbury University IT Department for assisting with these crime prevention tips.