A message from Attorney General Luther Strange

One of the most important jobs of the Attorney General is the protection of Alabama consumers. Our citizens need to be aware of scams that could cost them thousands of dollars or rob them of their identity. My office is working to empower and equip individuals with the information and tools to protect themselves against fraud and the criminals who prey on the unsuspecting.

In this brochure you will find information about cyber security. Learn the warning signs of online crime and protect yourself against these type of scams.

Sincerely,

Luther Strange

Alabama Attorney General's Office
PO Box 300152
Montgomery, AL 36130
334-242-7300

Important Consumer Protection Resources

Attorney General Consumer Protection Hotline
1-800-392-5658
www.ago.alabama.gov

Internet Crime Complaint Center
www.ic3.gov

Federal Trade Commission
1-877-382-4357
www.ftc.gov

Better Business Bureau
1-800-824-5274
www.bbb.org

Office of Cyber Security
Folsom Administrative Building
64 North Union Street, Suite 212
Montgomery, AL 36130
(334) 353-0722
www.cybersecurity.alabama.gov

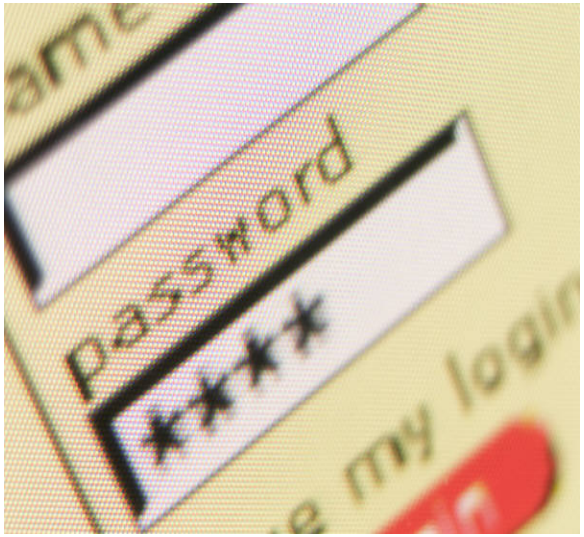
Attorney General Luther Strange
PO Box 300152
Montgomery, AL 36130
334-242-7300

Cyber Security: Protecting Your Online Information

Consumer Protection Contact Information:
Local: (334) 242-7335
Toll Free: 1-800-392-5658

COOKIES—WHAT ARE THEY? WHAT DO THEY DO?

- Internet cookies are small text files which are sent from a website to your computer each time you visit that website. These cookies are then stored on your computer for later use by that website, should you return to it.
- Cookies help websites "remember" each individual user and allow for an easier user-interface with the website.
- While useful in their purpose, cookies can pose a threat to your online privacy and security by compiling browsing history, identifying which state you are in, and exposing your personal information to potential hackers.
- Most modern browsers allow you to delete your cookies and/or completely disable your cookies.



CYBER SECURITY WARNINGS AND TIPS

- Never open any files, click on any hyperlinks, or download any material sent to you by strangers.
- Always back up all of your files on an external hard drive.
- Create strong passwords incorporating upper case and lower case letters, numbers, and symbols.
- An effective way to protect your computer and your information is to install a virus protection software. After installation, make sure the software is regularly updated. Many virus protection programs have the ability to automatically update.
- Use a firewall to block unwanted data from entering your computer.
- If you have to provide personal information over the internet, be sure that you are using a secured browser. A secured browser will display a "locked" padlock on the webpage, normally near the domain address at the top of the page.
- While file sharing programs or local computer networks will allow you to share files from one computer to the next, these programs and networks leave your computer vulnerable for hackers to access your files and personal information.
- Before disposing of your computer or hard drive, be sure to delete all personal information. Simply erasing the files or putting them in the "trash can" on your computer will not permanently delete them. You should use a "wipe" utility program to overwrite the entire hard drive before you dispose of your computer.

COMMON INTERNET THREATS & CYBER SCAMS

SMISHING or VISHING:

- In a Smishing (combination of SMS texting and phishing) or Vishing (combination of voice and phishing) scam, a victim will receive a text message or automated phone message describing an issue with the their bank account, credit/debit card, ATM card, or other personal information. The text message or phone message instructs the victim to text or call a certain phone number to "confirm" their personal information.

SPYWARE & MALWARE:

- Spyware and Malware are software programs that infect computers everyday.
- Spyware programs can monitor computer users and their actions, gaining personal information in the process. Spyware programs can also transmit a user's personal information to anyone or anywhere around the world.
- Malware programs interrupt computer networks and computer operations. These malware programs steal the information contained on the computer and sometimes make the computer inoperable.

STRANDED TRAVLER APPEAL SCAM:

- In a stranded traveler scam, victims receive an email from what appears to be one of their friends claiming to be stranded somewhere. The email states that the stranded traveler needs a certain amount of money wired to him so that he can return home. Never wire money to anyone without personally contacting them to verify that the transaction is legitimate.

Alabama Attorney General's Office
PO Box 300152
Montgomery, AL 36130
Local: (334) 242-7335
Toll Free: 1-800-392-5658