Protect Yourself Online

North Carolina Department of Justice

9001 Mail Service Center
Raleigh, NC 27699-9001

1.877.5.NO.SCAM
1.877.566.7226

www.ncdoj.gov

ATTORNEY GENERAL
JOSH STEIN

General Computer Safety

- Keep your operating system, spyware, virus protection software and firewall up-to-date.
- Use strong passwords for banking, shopping and websites that retain your credit card numbers, financial account numbers, or confidential information.
- Strong passwords have at least eight characters with a mix of upper/lower case letters, numbers and symbols (#, %). Don't use family names, consecutive numbers/letters, birthdays, anniversaries, etc.
- Consider a password manager so you only have to memorize one master password. Do research first with reputable reviewers to make sure it is best for you.
- For added security, consider using a two-step verification process (AKA Two-Factor Authentication, or TFA) when you log in to your devices or your high-security online accounts.
- Don't keep passwords or PINs in your wallet/purse, or written down next to your computer.
- Don't share passwords with others.
- If you compile a list of passwords or confidential financial information and store it on your computer, make sure the document is encrypted for extra protection.

Home Wi-Fi Safety

- Use a WPA2 router for added security.
- Password protect and encrypt your home Wi-Fi network. All networks, including WPA2, are subject to password attacks.
- Use a random password that is at least 20 characters long. (Note: You will only need this password when making changes to the network)
- For more on safer use of Wi-Fi including how to secure your home network's wireless router, search "NCDOJ Wi-Fi Safety."

Public Wi-Fi Safety

- Do not connect to networks automatically. Set your device to ask you if you want to join a public network.
- Avoid joining a fake network by asking a store employee for the correct Wi-Fi name and login. Do not assume that a network using "guest" or "public" is the correct network.
- Limit your Internet use to browsing and do not enter any sensitive information like account numbers or passwords.

Email Safety

- Never email or text credit card numbers, Social Security numbers or other confidential information. Encrypt or find a more secure way to pass along such private information.
- Avoid clicking on links in an email, even if it appears to come from a trusted source like your bank or a friend. To prevent triggering malware, type the URL link sent to you directly into the Internet browser rather than clicking on the link.
- Beware of email, texts, or social media posts that ask you to confirm your personal information or account number, even if the message claims to come from a company with which you do business. Instead, contact the business at a number or website you know to be valid.
- Forward fraudulent emails to spam@uce.gov.
- Emails that say you've won money, can make a lot of easy money, or plead for help are usually scams.

North Carolina Department of Justice

9001 Mail Service Center
Raleigh, NC 27699-9001

1.877.5.NO.SCAM
1.877.566.7226

www.ncdoj.gov

ATTORNEY GENERAL
JOSH STEIN

- Create an alternate email account to use when you make online purchases or when required to register first with unfamiliar Internet sites.
- Periodically check your spam filter settings and see what new security features your Internet service provider offers.
- If you suspect hacking or email tampering, report it to local law enforcement.

Social Networking Safety

- Limit information you make public on your profile and don't include your phone number, email or address.
- Be careful what you post. Some negative public posts about employers or classmates have led to lawsuits.
- Don't share when you will be away from home. Also, turn off geolocation for applications on your mobile devices.
- Use settings so that posts are seen only by friends or even specific groups of friends.
- It is safer to connect with people that you know in real life.
- People you know may have their accounts compromised. As with emails, be wary of links and attachments in messages.
- Keep your password private.
- Be wary of third party vendors on social media sites, especially if they ask for credit card information.
- Never respond to harassing or rude comments. Report comments to the networking site if they are bullying, unethical, criminal, or violate the site's terms of service.
- Under 18: Make your site private with limited access. Do not make visible your full name, school, cell phone number, address or email.
- Parents: Maintain access to your child's account. Set online time limits. Cellphones, tablets and other Internet devices should be kept in a family area even to charge overnight. Facebook & Instagram users must be 13 years old. You can report underage users anonymously.

Share Pictures Safely

- Think before you post. Once an image is posted on the Internet (even on a private profile), it essentially becomes public. It may never be completely erased from the Internet. Revealing photos sent to a friend may show up later to embarrass you.
- Control who can see your photos. Consider making certain photos or albums private.
- Under 18: Reduce identifying information in the backgrounds of pictures or video (i.e. school name, license plates, and street signs).
- When tagged in a photo, use security settings to ensure you approve the photo prior to it being shared with your friends.

Shop Online Safely

- Pay by credit card for a better chance of getting your money back if there are problems. Use a separate low-limit credit card for online purchases, or request a one-time-use number for each online purchase.
- Shop with online merchants that you trust. Research unknown businesses with our office, the NC Secretary of State, and/or the Better Business Bureau.
- Enter payment information only on secure sites. Look for https (instead of http) and a "lock" icon on the web address bar.
- Read refund and privacy policies before you order.
- Keep receipts or communications and a description of the product and its price until your order arrives and you've reviewed the charge.