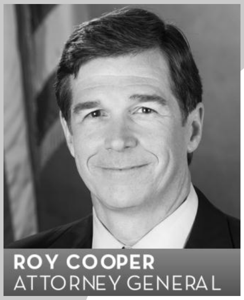
PROTECT YOURSELF ONLINE



ROY COOPER
ATTORNEY GENERAL

WI-FI SAFETY

Public Wi-Fi

- 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.

Home Wi-Fi

- 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."

PASSWORDS AND ONLINE BASICS

Keep your operating system, spyware, virus protection software and firewall up-to-date.

Use strong passwords for banking, shopping, or 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 words, names, consecutive numbers/letters, or 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.

BUYING AND SELLING

Pay by credit card. Federal law limits your liability for a lost or stolen credit card, and you have 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 from your credit card company each time you make a purchase online.

Shop with online merchants that you trust. Research unknown businesses with the NC Secretary of State, NCDOJ or the Better Business Bureau.

Look for https (instead of http) and a "lock" icon on the web address bar.

Keep receipts or communications, along with a description of the product and its price, until the product arrives and you've reviewed the credit card charge.

Read refund and privacy policies.

AUCTIONS: Read reviews about the seller and look for the number of transactions before placing a bid. Be wary if you're asked to complete a transaction outside of the auction site. Do not respond to sellers that contact you after the auction ends to purchase a product even though you didn't win the bid.

SELLING: When selling items online, watch out for fake checks and money orders. Contact the issuing bank, at a number you look up, to verify checks. Be wary of overpayments and endorsed checks. Never send "excess" payments back to the buyer or to someone else. Credit card payment is preferable.

Sellers should send items to physical locations, preferably to the address associated with the credit card.

ncdoj.gov

TIPS TO KEEP SAFE ONLINE

EMAIL

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. Verify with the friend or bank that they sent you the link first. To prevent triggering malware, type the URL link sent to you directly into the internet browser rather than clicking on the link.

Beware of emails (or texts) threatening something urgent and asking you to confirm your personal information or account number, or to transfer money. Don't call the number listed in the email. Contact the business at a number you look up.

Forward fraudulent emails to spam@uce.gov.

Hint: Emails that say you've won money, can make a lot of easy money, or plead for help are usually scams.

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

Limit your public profile information (phone, email, 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.

Limit posts to be 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 operating within social media, especially those requesting credit card information.

Never respond to harassing or rude comments. Hit delete. Report comments to the networking site if they are bullying, unethical, criminal, or violate that site's terms of service.

Under 18: Make your site private with limited access. Do not make visible your full name, school, cell, address or e-mail.

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.

PICTURES

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.

ONLINE SCAMS

Job hunting: Be cautious before providing your driver's license number, date of birth, or SSN.

Online dating: Never send money to someone you haven't met in person.

Do not click on pop-up messages or ads offering prices too good to be true.