SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS

CYBER SECURITY BASICS

Cybersecurity doesn't need to be complicated. Here are the basics of cybersecurity so you can be in control of your information and keep your devices safe.

PROTECT

Your Files & Devices

Update your software.

Outdated software makes it easier for scammers to hack your device. Set automatic updates.

Require passwords.

Use passwords for all of your devices. Don't leave these devices unattended in public places.

Secure your files.

Back up important files offline, on an external hard drive, or in the cloud. Make sure you store your paper files securely, too.

Use two-factor authentication.

This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.

Encrypt devices.

Encrypt devices, files and other media that contain sensitive personal information. Encryption protects information sent over your network so it can't be read by outsiders.

Your Wireless Network

Secure your home router.

Change the default name and unique password, turn off remote management, and log out as the administrator once the router is set up.

Setup a network firewall.

A firewall is a piece of hardware and/or software that protects and controls traffic coming into your network. If your router has a firewall option, enable it.

Use at least WPA2 encryption.

Make sure your router offers WPA2 or WPA3 encryption, and that it's turned on. Just like on your devices, the encryption will protect your info from being read/accessed by outsiders.

Disconnect old devices.

Disconnect older devices you no longer use from the network. Their security may be out of date, creating a weak point on your network.

Your Identity & Privacy

Own your online identity.

Every time you sign up for a new account, app, or get a new device, immediately set the information sharing privacy/security settings to what you're most comfortable with. Regularly check these settings to make sure nothing has changed.

Share with care.

Think before posting online. Consider what a post reveals, who might see it and how it might affect you or others. ID thieves use the information you post online to try and guess your passwords, security questions and/or steal your identity!

Beware of free Wifi hotspots.

Public Wifi networks are not secure, which means that anyone may see what you are doing while you are connected. Avoid logging into accounts like email and financial services. Consider using a virtual private network (VPN) or a personal/ mobile hotspot.

SHOPPING & SURFING ONLINE

We are online all of the time. Protect your info and money by considering these tips when shopping online:

Consider your payment options.
Using a credit card is much better than using a debit card; there are more consumer protections for credit cards if something goes wrong. If your debit card number gets stolen, that's a direct line into your bank account.

Monitor your statements.
Continuously check your accounts for any unauthorized activity. Set up alerts so that if your credit card is used, you will receive an alert with the transaction details.

Do your homework.
Scammers are good at setting up fake websites. Before making a purchase, read reviews. Look for a physical location, any customer service info and call the merchant to confirm that they are real.

Don't give it all away.
If the merchant is requesting more data than you feel comfortable sharing, don't shop there. You only need to fill out required fields at checkout and you should not save your payment information in your profile.

PASSWORD TIPS

There are a lot of ways to create a strong password, but here are the basics:

Make sure your password is at least 12 characters long with uppercase and lowercase letters, numbers and symbols. Avoid using common words, phrases or anything related to your personal life.

Pick security questions only you know the answer to and avoid using questions that answers could be easily found on the internet.

Don't reuse passwords or save your passwords in your internet browsers. Consider a reputable password manager if you struggle to remember your passwords.

Change passwords quickly if there's a breach. Change your passwords every three months to keep your accounts safe.

PHISHING SCAMS

Phishing scammers target consumers by sending them an e-mail, text or direct message that looks like it's from a trusted source. It asks for personal identifying information and then the scammer uses that info to open new accounts or invade the consumer's existing accounts. Some common ways scammers try to phish info from you include:

- Claim they've noticed some suspicious activity or log-in attempts.
- Say you must confirm personal information.
- Claim there is a problem with your account or payment information.
- Say you're eligible for a government refund or offer a coupon for free stuff.
- Want you to click on a link to confirm login information or make a payment.
- Include a fake invoice.

Remember! Never reply to calls, texts, pop-ups, or e-mails that ask for verification of personal information. Avoid clicking on links or downloading attachments from suspicious emails or texts.

IDENTITY THEFT UNIT
Education. guidance. enforcement.

To report a scam, visit www.consumer.sc.gov and click "How Do I..."

South Carolina Department of Consumer Affairs
293 Greystone Blvd., Ste. 400 • PO Box 5757 • Columbia, SC 29250
(800) 922-1594 • www.consumer.sc.gov

South Carolina
DEPARTMENT OF CONSUMER AFFAIRS