CRA
Transform IT
Computer Resources of America

What to know about CYBERSECURITY

PHISHING

An attacker will masquerade as a bank, organization, or service that they are not actually affiliated with. Their goal is to persuade you into opening up their email and clicking on a malicious link—this can lead to a download of malware, or a fake webpage. From there, they will try to steal your credentials and other private information.

PROTECTION

If you ever receive an email or text message that asks you to click on a link or open an attachment, make sure you have an account with the company, and do your research before ever opening anything that you don't recognize. You can protect your computer and phone by setting up security software that updates automatically, protect your accounts by using multi-factor authentication, and protect your data by backing it up regularly.

SPOOFING

Spoofing happens when a scammer impersonates a trusted and authorized source in order to steal data, private information, gain unauthorized network access, spread malware, and more. The attackers will try to act on trusted relationships by impersonating an organization that the victim is already familiar with.

PROTECTION

There are several different types of spoofing, and the easiest way to protect yourself is by simply contacting the organization or source in question. If you're ever asked to share passwords or credit card numbers, call the organization to confirm. Never open attachments you weren't expecting to receive, change your passwords regularly, and always confirm that you're on the company's real website.

MALWARE

Malware is software that sends viruses, worms, spyware, and more to damage or gain unauthorized access to a computer system. Once it gets in, the attackers can steal or delete sensitive information, alter computing functions, monitor activity without the victim knowing, and more. Commonly received through email, once the user opens a malicious attachment, it will be downloaded onto their computer.

PROTECTION

If you open an email and don't recognize the sender or the subject field is blank, make sure to never click on anything. Keep your software updated, backup files often, and consider purchasing enhanced security.