NCPC
National Crime Prevention Council

CLICK WITH CAUTION:
BE SCAM SMART

Online scams are on the rise. Be scam smart while browsing the internet. It's important to know what to look out for and what to do if you think you've been scammed.

PHISHING SCAMS

Scammers try to trick you into sharing sensitive information, like passwords or bank details, by impersonating legitimate organizations through emails, texts, or phone calls.

Don't take the bait

Always double-check who's sending you emails and never click on suspicious links. Never share personal information in response to an unsolicited email or text message. Criminals will often instill a sense of urgency to try to get your information quickly.

TECH SUPPORT SCAMS

Criminals may pose as technical or customer support and claim to have detected issues on your computer. They may ask for access to your device or payment for fake services.

Think twice

Legitimate companies will never call to offer tech support out of the blue. Hang up if you get one of these calls.

ROMANCE SCAMS

Scammers create fake profiles on dating apps or social media to establish relationships with victims. They use the illusion of a close relationship to manipulate or steal from them.

Go slow

Go slow and ask lots of questions. Research the person's photo to see if the image, name, or details have been used elsewhere. Trust your gut.

THINK YOU'VE BEEN SCAMMED? FOLLOW MCGRUFF®'S CHECKLIST AND...

STOP! Stop communicating with the scammer immediately if you're still in contact. Block them on any messaging platform, email, or phone number they've used.

CHANGE! Change your usernames and passwords for online banking, email, social media, and any other accounts. Use unique passwords for each account and enable two-factor authentication (2FA).

CONTACT! Contact your bank, credit card company, or cell phone provider to let them know you've been scammed. If the scam involved financial transactions, they can reverse the charge or freeze your account.

REPORT! Report the scam to your local authorities, the online platform, and the FBI's Internet Crime Complaint Center at ic3.gov.

SM

Sources: fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/tech-support-scams; usa.gov/scams-and-fraud