Most cybercrimes involve identity theft. Criminals steal personal information to hack accounts and access funds. Identity theft can lead to insurance fraud. Here are some common scams.

**Phone**
- Phishing: Scammers impersonate legitimate entities using malicious emails and texts to trick you into giving them your sensitive information. Suspect a phishing attack? Contact the proper organization directly to verify the request is real.

**Email**
- Formjacking: Cyber scammers hack a legitimate website to steal user information. Each time a customer fills out a form, a duplicate of the entered information is sent to the scammer. Contact the company if you suspect formjacking.

**Social Media**
- False Quizzes: Swindlers use surveys and quizzes to pry loose personal data. Launching a quiz app may give permission to pull information from your social media profile or phone, giving hackers an opening to steal your identity.

**Public Wifi**
- Using public Wi-Fi at coffee shops, libraries, or other locations puts you at risk for having information stolen. Avoid storing sensitive information on your phone and never share personal information over public Wi-Fi.

**Report**
- Report scams to your state consumer protection office.
- Online with the FTC complaint assistant.
- Fake websites, emails, malware, and other internet scams can be reported to the Internet Crime Complaint Center.
- Some online scams start outside the United States. If you have been affected by an international scam, report it through econsumer.gov.

www.InsuranceFraud.org