Be Wise to the Disguise

Prepare– know how to recognize a scam
Protect– personal information
Prevent– Identity theft and costly scams

Disguised as being helpful, a scammer can gain access to your personal information with just a few "friendly" questions. So, remember to keep your personal information safe:

Update Software– Outdated software is easier to hack and infect

Guard personal information– Things like Social Security numbers, bank account numbers, and even your address can be used to access accounts or open new ones

Protect Passwords– Don't share passwords with anyone and make sure all of your passwords meet recommended security standards

LSB

Lyndon
817 Topeka Ave
Lyndon, KS 66451
785-828-4411

Melvern
102 South Main
Melvern, KS 66510
785-549-3311

Topeka
1535 SW Fairlawn
Topeka, KS 66604
785-228-1133

FDIC
EQUAL HOUSING LENDER

Prepare Protect Prevent

- The most common scam is when a scammer sends you money under false pretenses, then requests some (if not all) of the money back for various reasons. This scam can present itself in various ways;
    - While applying for online scholarships some options ask you for your Remote Deposit information. After the scammers deposit the check using RDA, they request the money back for various reasons.
    - While buying or selling items online, scammers will contact you and offer to pay more than your asking price, on the condition that you send the difference back to them or a third party for shipping/handling fees.
    - YOU'RE THE BIG WINNER!! You are contacted out of the blue and the scammers tell you that you've won a large sum of money! All you need to do is cash the check and send some money back for processing fees.

BEWARE!! In all of these situations the check is most likely fake and you've paid the scammer using money you never truly had!

Never give out your account information unless it is a trusted and verified source and never negotiate a check on a strangers behalf.

- Don't be the victim of phishing! Phishing is a scam that uses fraudulent e-mails, appearing to be from a trusted source such as a financial institution or government agency. The e-mail directs you to a fake website that looks legitimate and asks to "verify" personal information.
- IRS Scams are on the rise! Usually IRS scams involve phishing and impersonations. Keep in mind the IRS will never;
    - Call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card, or wire transfer.
    - Demand that you pay taxes without the opportunity to question or appeal the amount they say you owe.
    - Threaten to bring in local police, immigration officers, or other law-enforcement to have you arrested for not paying your taxes. The IRS also cannot revoke your driver's license, business licenses, or immigration status.