Some tips to make you aware of potential issues you may face in this expanded networking world…(from BoA)

You're contacted unexpectedly

Watch for: A phone call, email, text, direct message or pop-up with a request for personal information or money.

Scammers will:

- Contact you out of the blue and claim there's an issue that needs immediate attention
- Ask for a favor, personal details, remote access to your devices or money.
- Try to confirm your identity with a verification code they send you – even though they called you.
- Insist you download apps or click links to "fix" issues or confirm information.

Remember: Scammers use convincing stories. They can use fake email addresses and Caller ID information – don't trust them.

Make sure you have verified the person who has contacted you before acting on any request. **Never click a link or download an attachment** from someone you don't know.

Bank of America will never text, email or call you asking for personal or account information. If someone reaches out and asks for it, it's a scam.

The communication plays with your emotions and pressures you to act immediately

Watch for: An alarming phone call, email or text. Someone is indicating there's a problem with your account, an issue with a delivery, an emergency with a loved one or product scarcity.

Scammers will:

- Pretend to be a loved one who needs help
- Pose as an employee from a familiar organization and say there's a problem that needs immediate attention
- Disguise themselves as a friend or love interest, even though they've never met you
- Claim to need money for emergencies, account problems, bills or travel
- Insist you keep quiet about the situation

- Tell you to not trust Bank of America or insist you respond to questions untruthfully.

Remember: Scammers use emotional triggers, like love, compassion, exhilaration or fear, to trick you into taking action. Do not act unless you have verified the person who has contacted you and the story or request is legitimate.

You're asked to pay in an unusual way

Watch for: A request for money. You may be directed to the nearest post office or a wire transfer service. Or, asked for bank transfers, pre-loaded debit cards, gift cards or virtual currency such as Bitcoin. They may send you a check and ask you to deposit it and use the deposited funds to do transactions.

Scammers will:

- Pressure you to pay with prepaid debit or gift card codes, wires, bank transfers or digital currency
- Send you a check for more than what is owed and tell you give the extra to someone else
- Have a reason for why you can't keep all the money

Remember: Many of these forms of payments are like cash and nearly impossible to trace or get back. Be wary when someone says you have to pay in unusual ways. Always verify who you're sending money to before you send it. Bank of America will never ask you to transfer money to anyone, including yourself, and we will never ask you to transfer money because we detected fraud on your account.

By law, banks must make deposited funds available quickly. The bank may make funds available, but that does not mean the check has cleared the paying bank or may not be returned unpaid as fraudulent at a later date. By the time the check is discovered to be fraudulent, the scammer has the money you sent and you may owe money to the bank for that check.

You're asked for personal information

Watch for: An unexpected phone call, email, text, direct message or pop-up with a request for personal information. This may be an account verification code, bank account number, PIN or social security number.

Scammers will:

- Contact you out of the blue
- Ask you to click links or open attachments to confirm your identity
- Coach you through steps to complete an action, like changing your password
- Use pop-ups on your computer or mobile device that ask you to allow software to run
- Provide a callback number or tell you to trust Caller ID when you question them
- Break into your mailbox to steal mail, especially checks
- Take you to a website that looks legitimate and asks for your login information

Remember: When in doubt, don't give it out. Never share account verification codes or personal information unless you've contacted the company through a verified method. Never provide strangers with remote access to your computer.

Bank of America will never text, email or call you asking for an authorization code. If someone reaches out and asks for it, it's a scam.