Protect Yourself Against Scams This Holiday Season

The holiday season is upon us—and so is the increase in scams occurring this time of year. Knowledge is power when it comes to protecting your identity, credit, or any of your financial assets from criminals' scams. At *Bank**Financial***, we're committed to helping you recognize scams so you can prevent falling victim to fraud or identity theft.

Here are some of the latest scams to be on high alert for:

Microsoft Takeover Scam

- Unsolicited Contact – Scammers contact you through fake popup alerts, unsolicited phone calls, or emails, falsely claiming to be from Microsoft. The takeover scam can include:
    - A claim there's a serious issue with your computer, such as a virus, a security threat, or a problem with a subscription.
    - A demand for remote access to your computer, often by having you install a program or click a link. Once they have access, they can install malicious software, steal your login credentials, or manipulate your financial information.
    - Financial Demands – They may charge you for fake services using gift cards, cryptocurrency, or other non-traceable payment methods.

Tip: Do not trust an unsolicited contact. Never call a number, click on links in popup alerts or emails, or engage a caller who claims to be from Microsoft trying to fix a problem. And **NEVER** grant a stranger remote access to your computer.

Note: Similarly, the Social Security Administration (SSA) will **NEVER** contact you to 1) threaten you with arrest or legal action, 2) suspend your social security number (SSN), or 3) demand immediate payment from you. Scammers use these tactics to scare you into providing personal info or money.

Scams Using Artificial Intelligence (AI)

- Deepfake Video and Voice Clones – Scammers use AI to impersonate someone you trust in a seemingly realistic video call or voice message.
- Phishing Emails – AI-written emails that appear so real you may not spot phishing.

Tip: Verify via another channel (e.g., call or text) if someone is urgently asking for money or sensitive info—especially via video or voice.

Pig-Butchering Investment Scheme

- Building "Trust" – Like taking "pigs to slaughter," fraudsters build trust over time (e.g., via dating apps or social media), then lure you into making fake cryptocurrency investments. The scammer continually wants more money to "grow" the investment—until you discover you can't withdraw.

Tip: Beware of "too good to be true" investment opportunities, especially in crypto. Don't send money to platforms or individuals you haven't vetted.

Employment / Job Scams

- Fake Job Postings – Scammers impersonate real companies or recruiters, asking for "upfront fees" for training, certifications, etc. Some may trick you into downloading malware disguised as "recruitment software" or interview tools.

Tip: Never pay to get a job, always verify the company independently, and don't download software without checking its legitimacy.

Investment Scams (Beyond Crypto)

- Traditional Investment Scams – Fake "high return" opportunities, Ponzi-style schemes, etc. Scammers may show "proof" of returns (fake statements) to build trust, then disappear when you try to withdraw.

Tip: Vet any investment opportunity carefully (do research; ask questions). If something feels off, don't send money.

Credit / Debit Card Fraud

- AI and Bots – Fraudsters use these to automate attacks targeting mobile payment apps and online sites.
- Synthetic Identity Fraud – This growing scam creates "fake" identities using real and fabricated info.

Tip: Enable account transaction alerts, use strong authentication, and monitor statements.

Insurance Fraud Powered by AI

- "Doctored" Claims – AI is enabling new kinds of insurance fraud—such as fabricating accident photos/videos to support false claims.

Tip: As a consumer, be mindful of "too good to be true" insurance deals; make sure you document everything when filing a claim.

Elder Exploitation via Impersonation

- Imposter / Impersonation Scams – Scammers target older adults by impersonating someone else, sometimes using AI deepfake (e.g., "I'm your grandchild in trouble"). Imposters posing as government and businesses continue to be one of the biggest loss drivers.

Tip: Discuss risks with older family members, ask them to verify urgent money requests with a trusted person, and help them enable account safeguards such as fraud alerts.

To learn more about how to recognize scams and ways you can prevent fraud, visit our website **www.bankfinancial.com/fraud-security**.