How to prevent deepfake scams

Deepfakes are a new and serious threat. Using artificial intelligence, scammers can create hyper-realistic fake videos, images, and audio of people to trick you. They might clone a loved one's voice in an emergency call, impersonate your boss in a video conference to demand a wire transfer, or even create a fake video of a celebrity to promote a fraudulent investment. Staying safe from deepfakes is all about being a little more cautious and trusting your instincts. Check out these helpful tips to safeguard your money and personal information.

Trust, but always verify

This is the golden rule for deepfake protection. If you receive a request that seems urgent, emotional, or out of character, don't act immediately.

- **Financial requests**: If you receive a call, text, or email from someone - even if it sounds or looks like a person you know - asking for money, a wire transfer, or sensitive account information, stop and take a moment.
- **The "secret password" trick:** Create a "code word" or "safe word" with close family and friends. Just like we do when you call in for account information, if someone calls with an emergency, you can ask for the code word to confirm it's really them.
- **Use a second channel:** Hang up the phone or close the video call and contact the person through a different, verified method. Call them back on a number you already have saved, or send a text message. Don't use the phone number or contact information provided in the suspicious communication.

Protect your online footprint

Scammers create deepfakes using your online photos, videos, and public information, but you can reduce the amount of material they have to work with.

- **Tighten your privacy settings:** Make your social media profiles private and restrict who can see your posts. Be mindful of the photos and videos you share of yourself and your family.
- **Be cautious of unsolicited connections:** Be careful about who you accept as a "friend" or "follower" online. Scammers may try to connect with you to gather information.
- **Consider watermarking:** If you post high-quality photos or videos online, a simple digital watermark can make it harder for scammers to reuser your content.

Learn to spot the red flags

While deepfakes are getting more sophisticated, many still have subtle flaws. Be on the lookout for these signs:

- **Unnatural audio:** Listen for strange pauses, a robotic or flat tone, weird intonations, or poor lip-syncing in videos.
- **Visual oddities:** Look closely at the video. Does the person's face look slightly off or detached from their body? Are there inconsistent shadows, lighting, or skin tone? Does their hair look unnaturally perfect? Are their eyes blinking strangely or not at all?
- **The "too good to be true" test:** Be skeptical of any video or audio that seems outlandish or offers a prize or an easy investment. Scammers often use deepfakes to create urgency and manipulate your emotions.

Strengthen your digital security

Your best defense against any scam is robust digital security.

- **Multi-factor authentication:** MFA is one of the most effective ways to protect your accounts. It requires a second step to log in, like a code sent to your phone or a facial scan. This makes it much harder for a scammer to access your accounts, even if they have your password. Enable MFA on all of your financial, email, and social accounts.
- **Strong, unique passwords:** Use long, unique passwords for every account. Consider using a password manager to help you remember them all.
- **Keep software updated:** Turn on automatic updates for your devices and software. These updates often include critical security patches that protect you from the latest threats.
- **Beware of phishing:** Deepfakes are often used in phishing attacks. Don't click on suspicious links or download attachments from unknown sources.

REMEMBER: We're here to help! If you have any questions or think you may be a victim of fraud, reach out to your Business Banker, Relationship Manager, or visit your nearest Branch.