View as Webpage

Protect Yourself Against Deepfakes

We want to make you aware of a growing threat called "deepfakes." These are fake videos or audio clips created using artificial intelligence that can make it seem like someone is saying or doing something they didn't. Deepfakes can be used for identity theft and fraud, so it's important to know how to protect yourself.

Here are some simple steps you can take to safeguard your personal information:

- Be Careful What You Share: Avoid posting too much personal information online, especially high-quality photos and videos. Adjust your privacy settings to limit who can see your content.

- Use Strong Privacy Settings: Make sure your social media and photo-sharing accounts have strong privacy settings. Restrict access to your personal data and reduce what is publicly available.

- Watermark Your Photos: Consider adding a digital watermark to images you share online. This can help deter misuse of your content.

- Stay Informed: Keep up with news about deepfakes and AI. Being aware of these technologies can help you spot suspicious content.

- Enable Multi-Factor Authentication: Use extra security steps for your accounts, like a code sent to your phone or a fingerprint scan. This makes it harder for unauthorized users to access your accounts.

- Use Strong Passwords: Create unique, long passwords for each account and use a password manager to keep track of them.

- Keep Software Updated: Regularly update your devices and software to protect against security vulnerabilities.

- Beware of Phishing: Be cautious with unknown messages or calls asking for personal information. Verify the sender's identity before clicking on links or sharing details.

- Report Suspicious Content: If you encounter deepfake content involving you or someone you know, report it to the platform hosting it and to federal law enforcement.

- Seek Legal Advice if Needed: If a deepfake damages your reputation, consult with cybersecurity experts and consider contacting your elected representatives to advocate for stronger regulations.

- By staying informed and following these guidelines, you can better protect your digital identity from deepfake threats and other cyber risks.

For additional security information, you can visit Oak Bank's Security Information on our website.

Oak Bank will never ask for personal information over an unsolicited phone call, text, email, or online chat. Never share your account information, PIN number, username/password or one-time password.

If you receive an unsolicited phone call or text message requesting your Oak Bank account information, report it immediately by calling 608.441.6000 or sending an email to bank@oak.bank.

Need help with your account?

Email: bank@oak.bank
Call: 608.441.6000

If your Oak Bank Debit/ATM Card has been misplaced, call 877.755.2957..

If you have misplaced your Oak Bank Visa Credit Card, call 800.423.7503.

Visit Oak Bank Online

608.441.6000
877.625.2265 Toll Free

Lobby
M - F: 8 a.m. - 5 p.m.

Drive-up
M - F: 8 a.m. - 5 p.m.

Member FDIC

STAY CONNECTED

This Oak Bank message may contain promotional content.