Stay Safe Online:

Protect Yourself from Cyber Threats.

Whitefish CREDIT UNION

WhitefishCU.com | 406-758-0430

04/2025

Watch Out For Phishing Scams

Scammers use email (phishing), phone calls (vishing), and text messages (smishing) to trick you into revealing personal information.

Be on the lookout for:

- **Urgent Requests** — Messages claiming your account will be suspended unless you act immediately.
- **Threats & Fear Tactics** — Blackmail, legal threats, or demands for payment.
- **Suspicious Links or Attachments** — Unfamiliar emails urging you to click or download.
- **Generic Greetings & Odd Email Addresses** — Messages that feel impersonal or slightly "off."

If you suspect phishing:

- ✗ Don't reply, click links, or open attachments.
- ✓ Verify by visiting the official website or calling the company directly
- ✓ Delete or report suspicious messages as spam.
- ✓ Never trust caller ID alone—if something feels wrong, hang up and call the official number.

Keep Your Devices Secure

1. Update Regularly

Keep your phone, computer, and apps updated. Windows 10 support ends in October 2025!

2. Use Strong Passwords

Create long, complex passwords or passphrases. Avoid reusing passwords.

3. Enable Multi-Factor Authentication

Over 90% of hacked accounts didn't have MFA enabled. It's a simple but powerful security layer.

The Rise of AI: How Scammers Are Using It Against You

Artificial Intelligence (AI) is a powerful tool that can create realistic images, voices, and even entire conversations. While AI has many benefits, it has also made scams and cyber threats more convincing and widespread.

- **AI-GENERATED PHISHING EMAILS:** Messages that look legitimate but aim to steal your data.
- **DEEPFAKE VIDEOS & VOICE CLONING:** Scammers impersonate real people to gain trust.
- **AUTOMATED SCAM CALLS & MESSAGES:** AI-powered bots send realistic texts and voicemails.
- **DATA HARVESTING:** AI gathers personal details from social media to create targeted scams.

> AI is evolving fast, and so are scams.

How to Protect Yourself

Be skeptical of unexpected requests for money or sensitive information. Even if they appear to come from someone you know.

Verify before you trust! If a video, email, or phone call seems suspicious, confirm with the real person through another method.

Avoid sharing personal details online that could be used in AI-generated scams.

Think before you input sensitive data into AI tools. Platforms can store and use your information.

Stay alert, stay informed, and protect yourself!

Visit WhitefishCU.com/Security for more tips.

Whitefish CREDIT UNION