There are many legitimate and useful purposes for artificial intelligence (AI) technology, but it's also being exploited by criminals. These bad actors are now able to impeccably fake the voices and faces of people you know and pretend they are in distress in an effort to steal your money or identity.

To protect yourself from these high-tech voice scammers:

- **Consider choosing a safe word for your family.** Share it only with family members or others in your inner circle. If someone calls claiming to be a grandchild, for example, you can ask for the safe word or words and if the caller doesn't know it, it's clearly a scam.
- **Call back your "grandchild" in crisis.** If you don't have a safe word and your supposed grandchild or child calls saying there's a medical emergency or some other crisis (sometimes callers say they've been kidnapped), they may add that their phone is broken so you can't call them. Pause, take a breath (criminals try to rattle you to disrupt your rational thinking), and tell them you want to try to call them back anyway. Chances are your real grandchild will pick up, unharmed and bewildered by your concern.

Facebook Isn't Always Friendly

Facebook can be an extremely valuable platform for connecting with friends and family, but its popularity can make it a prime stalking ground for scammers. The potential risks to your personal information can be significant, with fraudsters using various tactics, from clickbait schemes to Facebook marketplace and fundraising scams.

1. Clickbait scams

A clickbait Facebook scam involves an exaggerated or misleading headline to attract your attention. The bait could be anything from sensational fake news about a celebrity to an unbelievably good deal on a popular product. Once you click these links, you might be redirected to malicious websites or inadvertently download malware.

2. Fake prizes and giveaways

Victims of fake prizes and giveaways receive notifications that they've won a prize they never entered, such as a lottery, sweepstakes, or contest. The catch is that before the prize can be claimed, scammers usually request personal information or payment to cover supposed taxes, processing fees, or shipping costs. Cybercriminals can then use the information captured for identity theft or further scams.

3. Fake "free" listings

Fake "free" listings are a Facebook Marketplace scam that aims to lure you in with the promise of obtaining goods or services at no cost. However, these listings often lead to hidden fees, deceptive practices, or outright fraud. Scammers may ask you to provide personal information, pay for shipping or handling, or request other unexpected charges.

Sellers need to be aware of buying scams, too, like overpayment scams. Whether you're

a buyer or seller, always keep payment on Facebook Marketplace and don't agree to a transaction over a payment app, gift card, etc.

4. Charity and donation scams

Charity scams exploit goodwill and encourage urgent donations to a cause. They can be for an invented cause or pretend to be raising money for a real disaster, someone battling an illness or a humanitarian crisis. They often request personal information or payment through unconventional methods like gift cards, which are difficult to trace. If you want to donate to a charity, do so through their official website.

5. Video scams

Video scams involve distributing an enticing video that makes a victim want to click to view it. These scams trick users into clicking infected links or downloading attachments. One example is when you get a message saying, "Is it you in this video?" which can come from a stranger's account or a hacked friend's account.

Don't be tempted to click through. If it came from a friend's account and the curiosity is too much, contact them via another channel to make sure they sent it, and their account hasn't been compromised.

Protect Yourself from Facebook Scams

Follow these tips to help keep your personal information safe and reduce your risk of falling for a scam on Facebook:

- **Decline friend requests from unknown people:** Only accept friend requests from people you know and trust.
- **Avoid clicking suspicious links:** Be cautious when clicking links or downloading attachments, which may lead to malicious websites or malware infections.
- **Turn on Facebook's login alerts:** Enable login alerts to receive notifications whenever someone logs into your account from an unrecognized device or location.
- **Adjust your online privacy settings:** Review your privacy settings and limit who can see your posts and personal information.
- **Use Facebook's "Security Checkup" tool:** This tool helps you assess your account security and identify potential vulnerabilities.

Remember to stay vigilant, be cautious of suspicious activity, and prioritize your online security.

Don't Believe Everything You Read (or Hear)

According to the Federal Trade Commission, scams that impersonate well-known businesses and government agencies are consistently among the top frauds reported to their Consumer Sentinel Network. Impersonation scams are initiated by a person who pretends to be someone you can trust to access your sensitive data or steal money from you via email, text message, social media, or phone call.

Phone Scams

Phone scammers can target you by calling directly using robocalls, by spoofing legitimate numbers or a combination of the two. The easiest way to avoid a phone scammer is to not pick up calls from numbers you don't recognize. If it's a legitimate call, they will leave you a message.

If you do answer a call from an unknown number, hang up immediately if anything seems suspicious. These types of criminals often pretend to work at real companies, and they offer detailed backstories and may have knowledge of your activity with the legitimate company so be wary of what your caller ID says. Information can be spoofed to make these scammers seem legitimate.

And NEVER give out any personal or company information (like your address, last four digits of your social security number, or other sensitive details) no matter how legitimate

an unsolicited call may seem.

Enriching the Lives of Members Over 50

The National Council on Aging reports that senior centers are one of the most widely used services available to elders in America. Community centers that serve elders over the age of 50 are locally funded but may also receive State and Federal grants. Some senior centers have a small membership fee, which may be waived based on your income.

Senior centers provide:

- Meal and nutrition programs (ex: the Meals on Wheels Community Cafe)
- Health & Wellness programs
- Information on community resources
- Eligibility screening for Local, State & Federal assistance programs
- Assistance identifying employment or volunteer opportunities
- Limited transportation

Check out Senior Centers in Rhode Island to find a center near you.

Email and Text Scams

Phishing emails are among the most common impersonation scams. They are designed to trick you into divulging sensitive information like your checking account information or social security number. In **pharming scams**, someone attempts to install malware or some type of malicious code on your electronic devices.

Here are a few tips and tools to avoid falling prey to email scams:

- NEVER click on attachments or respond to emails from sources you aren't sure about. Just delete them from your inbox.
- Use multi-factor authentication on your devices to add an extra layer of security when logging into your online accounts or websites that contain sensitive information like online banking and bill paying.
- Use antivirus security software to eliminate many security threats. Get an annual subscription to help protect your emails and web presence.
- Back up your data often. Should the worst happen, it will make your recovery efforts simpler.

Scams that target you via **text message** work similarly to email scams. The best way to avoid falling prey to these attacks is to NEVER click on links sent to you from a phone number you do not recognize.

Bank Impersonation Scams

A bank impersonation scam is when someone reaches out pretending to work at a credit union or bank you use, either to steal your credit or debit card information, get you to hand over money, or to get around your credit union's security protections to access your PINs.

Contact us:

Email: memberservice@peoplescu.com

Phone: 800.498.8930

Follow Us:

To learn more, check out our Fraud and Security Archive. If you fall victim to an impersonation scam and encounter fraudulent activity related to your PCU account, contact Erine Lewis, Head of Risk, immediately at 800.846.8930.

We're Here to Help. Stay alert, trust your instincts, and remember that People's Credit Union is always here to support your financial security. If you encounter suspicious activity, report it immediately. Together, we can outsmart fraudsters and protect what matters most.