Take Care of YOU

A Health and Wellness Bulletin | October 2024

Protect Yourself from Common Scams

Scams are deceptive schemes designed to defraud individuals or organizations of money, personal information, or other valuables by exploiting trust and manipulating emotions. The digital space presents numerous opportunities for fraudsters, and scams can take many forms, including but not limited to:

Online scams: Examples include phishing emails, fake websites, and social media fraud. Scammers may impersonate legitimate companies to acquire personal information or money. **Phone scams:** These scams involve calls from people claiming to represent reputable organizations, such as banks or government agencies, and they may request sensitive information or payments. **Hostage Phone Scams:** Scammers claim to have taken a loved one hostage, demanding immediate payment through untraceable methods like wire transfers or gift cards. **In-Person Scams:** Scammers approach victims directly, often posing as service providers or charity workers and using high-pressure tactics to solicit money. **Investment Scams:** These involve schemes that promise high returns on investments with little risk, often leading people to lose substantial amounts of money. **Prize Scams:** Victims receive messages claiming they've won a lottery or prize but must pay a fee to claim their winnings. **Relationship Scams:** Scammers build online relationships with people, eventually asking for money under various pretenses. **Tech Support Scams:** These scammers impersonate tech support representatives and claim that there are issues with the person's computer, leading them to provide access or pay for unnecessary services.

To protect yourself from scams, trust your instincts—if something seems suspicious or too good to be true, it likely is. If you are targeted by a scam, try to stay calm, avoid giving personal or financial information, and end the communication immediately. Verify the scammer's claims by contacting the relevant person or organization directly, and report the incident to authorities like the Federal Trade Commission (FTC) or local police. If you've shared financial details, contact your bank to secure your accounts. Taking these precautions and educating your loved ones can help prevent you and others from becoming the victim of a scam.

Cybersecurity Resources

- National Cybersecurity Alliance (NCA)
- Cybersecurity & Infrastructure Security Agency (CISA)
- Federal Trade Commission (FTC)
- SANS Institute
- Microsoft Security Blog
- Google Safety Center
- Electronic Frontier Foundation (EFF)
- Norton Cybersecurity Center
- Stay Safe from Phishing - Google Phishing Quiz