



ELDER FINANCIAL EMPOWERMENT PROJECT

Scams: Are you Prepared?

Contact –

Sonia Komisar | Victim Services Attorney
Elder Financial Empowerment Project

Phone (608) 224-0606

Email: skomisar@cwag.org

www.cwag.org

The Elder Financial Empowerment Project provides services statewide to victims at least 60 years of age who have been financially exploited, abused by a fiduciary, scammed, or had their identity stolen.

This project is supported by the Victims of Crime Act Subgrant No. 2021-VO-A/VO-01 18970 awarded by the Wisconsin Department of Justice Office of Crime Victim Services under a grant from the US Department of Justice Office for Victims of Crime.

We do not discriminate based on age, race, ethnicity, national origin, religion, gender, sexual orientation, disability, medical history, or other non-merit characteristics.

Who Do We Serve?

- Victims of financial exploitation/abuse 60 years of age and older
- Statewide service
- Free legal services
- No income or asset restrictions
- Entirely confidential
- Not a mandatory reporter

The Services We Provide to Victims of Financial Exploitation

- Consultations
- Stabilization
- Advocacy and representation
- Revictimization Prevention
- Outreach



ELDER FINANCIAL EMPOWERMENT PROJECT

Prizes, Lottery, and Sweepstakes Scams

Telephone or email congratulating recipient on winning a lottery, drawing or sweepstakes! Usually something the victim hasn't entered. "Winner" asked for **upfront payment** to cover processing fee, taxes or postage.

Sometimes a letter, "claim certificate" or "check" as **an advance** to cover the above costs. Check doesn't

Sweepstakes Recovery Scam

Follow up scam to sweepstakes scam. When winnings don't arrive, victim is contacted by **a person claiming to be an attorney** that will represent the sweepstakes "winners".

Advance Fee Loans

Scammers will target people looking to apply for a loan or credit card, offering their service regardless of credit history. Scammers will then ask the victim to pay some kind of fee, usually labeled as a **processing, insurance, or application** fee. If you hear these words used in this context, it's a scam.

What can you do?

Do not pay advance fees for credit card or a loan!

How to avoid

Legitimate sweepstakes are free and do not require a wire-transfer.

Never agree to pay to claim a prize or a gift.

If they request that you wire them money –IT is a SCAM, end the transaction immediately.

Keep credit card and bank account numbers safe and private-avoid sharing.

Information may be requested during an unsolicited sales pitch and could be used to access and empty bank accounts.

Resist any pressure to "act now".



ELDER FINANCIAL EMPOWERMENT PROJECT

Internet & Computer Scams

Spoofting

When receiving a phone call, text, or email be wary. The caller ID or email may have been 'spoofed' to look like a trustworthy company or even someone you know. Scammers often block their real identities in order to get you to open or respond, which can infect, destroy, or otherwise harm your computer/phone. And steal your sensitive information.

Phishing

Scammers create authentic-looking emails, text messages and internet pages to entice victims to disclose financial information. You may also experience a computer problem screen pop up allegedly from Microsoft or Google offering to charge a fee to "fix" detected problem. These are both common examples of scammers 'phishing'.

Tips to avoid phishing:

- ❗ **Do not click links** in unsolicited emails.
 - ❗ **Do not open attachments** until confirmed with company.
 - ❗ **Do not click on pop-ups** that appear as internet ads on your computer and change your browser settings to block pop-ups.
 - ❗ **DO NOT RESPOND** instead contact company directly using their legitimate number from your paperwork, not the number provided by the scammer.
- Grammatical errors are a red flag** that the email is not from a professional, reputable, and legitimate business.

Tips for...

Spoofting

Delete messages from unsecured sources without opening or responding to the messages.

Fake QR Code Scams

QR Codes such as this:



may be altered to contain malicious code so when scanned, scammers can access to your mobile device revealing your location and forfeiting access to personal and financial data.

Do not download apps or send payment through QR codes.



ELDER FINANCIAL EMPOWERMENT PROJECT

Home Improvement Scams

Contractor Fraud

Some contractors use **high pressure tactics** for **unnecessary or overpriced contracts**, then deliver **shoddy work**. Once they start, they often “find” other work that needs to be done urgently—often in areas that victim cannot access themselves to inspect what is needed and what has been done.

Unsolicited Work

Victims **coerced, intimidated, or conned** into paying **unreasonable amounts for poor quality work** for services such as roofing, paving, auto body repair etc. Work usually paid for but **work never started** or of such **poor quality** that victim must often have to pay to have scammers work corrected.

How to avoid home improvement scams

- **Try** to hire a local contractor.
- **Call** the Better Business Bureau to research the contractor.
- **Confirm** that a contractor is registered and bonded.
- **Get references** and check their credentials by looking up the company.
- **Get two to three written estimates** before choosing a contractor.
- **Get all** estimates, contracts and warranty **information in writing** including a start and completion date, what work is to be done and materials to be used.
- **Know** whether the contractor will be subcontracting your job and **who will be doing the work**.
- **Get lien waivers** from anyone that you pay for home repairs.
- **Never pay with cash** or checks made out to cash.
- **Beware** of contractors promising to pay or rebate portion of an insurance deductible as an incentive to contract.



ELDER FINANCIAL EMPOWERMENT PROJECT

Imposter Scams, Romance Scams, and more

Imposter Scams

Scammers often misrepresent who they are in order to obtain your sensitive information. Some may try to elicit your Credit Card Account confirmation, pretend to be Social Security Administration notifying you of a problem with your SS number, pretend to be IRS or US Treasury Dept. and threaten you to pay now under threat of arrest, notify you a utility service disconnection is imminent, or pretend to be Law Enforcement – alleging there is an outstanding warrant for your arrest.

Fictitious Relative/Grandparent

Imposter calls claiming to be grandchild or relative who has been arrested travelling or stranded while traveling – might need wire transfer for bail, emergency car repairs or a medical bill. Often doesn't want "mom or dad" to know.

AND BEWARE: New artificial intelligence allows scammers to sound just like family.

Romance Scams

Perpetrator enters the victim's life as a romantic interest in order to gain influence and eventual financial control. Often requests for money for travel costs, medical bills for self or for family members. When asked to meet, they always have more problems with travel requiring additional money before can visit.

Do not cash checks for them. **Be wary** of anyone online who immediately professes their love for you, repeatedly gives excuses for not meeting in-person, or anyone who asks for your sensitive information. Be safe!

What to do...

Imposter Scams

- Do not trust Caller ID. Information could be spoofed (phone number is misrepresented).
- If you receive a call or email that you are not expecting—CHECK IT OUT!
- Never give a caller access to your computer.
- Never pay by wire transfer or by pre-paid debit or gift cards. Hang up on the call or delete email.
- Government does not make unsolicited calls.

Fictitious Relative/Grandparent

- Ask personal questions to verify the caller's identity using questions only a close family member would know.
- Do not fill in the blanks for the caller.
- Contact your grandchild using a number you know and if they can't be reached contact another family member.
- NEVER wire money to scammers.