Senior Savvy: Wise Owls Navigating Cyber Scams

Written By Angela P. Doughty, CIPP/US (apd@wardandsmith.com) and Sydney C. Smith (scsmith@wardandsmith.com)
December 6, 2023

As the relentless march of technology continues, scams have evolved into cunning traps, presenting a challenge to individuals of all ages.

Among the great tapestry of age groups, despite the wealth of experience and wisdom gained from navigating life's journeys, our wisest are often the most susceptible to the cunning tactics of the sly-as-fox scammers.

In our digital world where scams lurk behind every pixelated tree, many wise owls perch cautiously on the branches of technology, hesitant to embrace it fully, fearing their nest eggs being pilfered. But fear not, though wary, we can still hoot with knowledge in the face of these modern-day challenges.

Digital Nest Defense

To protect against financial fowl play, there are measures wise owls can take to evade and remain alert against the crafty schemes of deceitful predators.

1. **Enlightenment:** Delve into the depths of knowledge! Familiarize yourself with common scams by attending seminars, watching videos, or reading up on scam-busting articles from reputable sources, such as the AARP Fraud Watch Network or the Federal Trade Commission (FTC). And don't forget to tap into the wisdom of the younger flock for insights on new digital branches.

2. **Fortify Secrets:** Guard your nest – never share personal or financial information over the phone, email, or text unless you initiated the contact and are certain of the recipient's identity. Always keep reputable computer anti-virus and security software updated. And passwords? Use unique, varied passwords for all accounts that are as unyielding as talons.

3. **Verify Before You Trust:** Scammers often pose as government officials, bank representatives, charity organizations, phone companies, and even family members to gain trust and access to personal information. Be skeptical and ask questions. Take flight to verify the callers' credentials by independently checking the website or directly contacting the supposed institution or individual – do not use any contact information provided by the unknown caller, texter, or emailer. When in doubt, silence is golden, as bad actors will move on if you do not engage.

4. **Avoid Unsolicited Contact:** Any unsolicited contact from a 'bank representative', 'government official', or other formal request for personal information should ring alarm bells. And those suspicious emails with tempting links and attachments? Don't click, don't open, and delete. They're like tangled...
branches in a storm – better to avoid.

5. **Play It Cool**: Scammers love to ruffle feathers with high-pressure and emotional manipulation tactics – often urging immediate decisions and payments or threatening criminal liability for failing to take the requested action or provide the requested information. Take the time needed to check all requests independently of the potential scammer. Time is your ally; don't rush to land on uncertain perches.

### Wise Owl Warnings

Even the most astute owl might find themselves tangled in the web. Keep your eyes sharp, and watch out for these red flags.

1. **Too Good to Be True**: Remember, if it sounds too good to be true, it probably is. Those flashy offers, large sums of money, or once-in-a-lifetime investments? Stay cautious and be skeptical of these opportunities, and get more information before making a decision. Trust your instincts and seek the wise counsel of loved ones and professionals.

2. **Demanding Personal Information**: Exercise caution regarding any uninvited requests for sensitive details, like Social Security numbers, banking particulars, or credit card information. Legitimate requests from known institutions and individuals will adhere to established protocols – they will not request entry to your treehouse without a valid purpose and will be respectful of independent verification requests.

3. **Odd Payment Methods**: Be wary of requests for payment via gift cards, wire transfers, or cryptocurrency. These are like foreign birdcalls. Legitimate institutions generally do not request or accept these payments.

4. **Tech Support Shenanigans**: The tech support calling claiming your computer's possessed? Hang up! Computer frozen with a number to call to unlock it? Hold your perch! Don't let anyone uninvited swoop into your digital nest. Independently engage all technical support services.

5. **Charity Charades**: Be cautious when donating to charities. Verify the legitimacy of the organization and try to donate through the official website or mailing address when possible. Scammers love to disguise themselves in the feathers of kindness. Stick to the beaten path for donations.

### Fallen Victim

Even the most astute owl may find itself ensnared. In such a situation, swift action akin to the breeze weaving through branches is crucial:

- Cease all interactions with the hacker and promptly change the logins, passwords, and PINS for all accounts containing personal or financial data.
- Complete the FTC Identity Theft Report (gov). An FTC Report will help you (i) remove fraudulent information from your credit report; (ii) stop a company from collecting debts that result from identity theft or from selling the debt to another company for collection, (iii) extend the fraud alert on your credit report; and (iv) get information from companies about any accounts the identity thief opened or misused.
- File an FBI Internet Crime Complaint (IC3) to report that you have been the victim of an Internet crime. Internet crimes involve the use of the Internet to communicate false or fraudulent representations, including advance-fee schemes, non-delivery of goods or services, computer hacking, or employment/business opportunity schemes.
- File a police report with your local law enforcement agency (police, sheriff).
- Obtain a credit report and request a one-year fraud alert by reaching out to one of the three credit bureaus.
Contact the fraud department of any business, credit card company, or financial account flagged by the hacker, or that should not be reflected in the credit report.

Retain documentation of all correspondence, reports, and filings and consider implementing an extended fraud alert or credit freeze through one of the credit bureaus.

By arming ourselves with knowledge and taking proactive steps to outsmart these scammers, we can soar through the digital sky with confidence, knowing our nest eggs are safe. Stay connected with family members, friends, and trusted advisors who can provide support and guidance in recognizing and addressing potential scams.

If you have questions about how to best protect yourself from fraud, please reach out to our Trusts and Estates and Privacy Law attorneys. We’re here to help. Contact a team member today.

--

© 2023 Ward and Smith, P.A. For further information regarding the issues described above, please contact Angela P. Doughty, CIPP/US or Sydney C. Smith.

This article is not intended to give, and should not be relied upon for, legal advice in any particular circumstance or fact situation. No action should be taken in reliance upon the information contained in this article without obtaining the advice of an attorney.

We are your established legal network with offices in Asheville, Greenville, New Bern, Raleigh, and Wilmington, NC.