It's All About Money: How to Spot a Scam

Wendy C Kasten, AWWC Chair

Jeff Trafton, Sheriff, Waldo County, Maine

Scammers target everyone. They target people of all ages, backgrounds, education levels and income levels. There are entire buildings and businesses in some countries devoted to dreaming up scams, and ways to get money out of what the scammers perceive to be wealthier countries.

The best defense against scammers is your ability to recognize when someone is attempting to scam you. Develop your scam recognition skills. When dealing with uninvited contacts from people or businesses, whether it's over the phone, by mail, e-mail, in person or on a social networking site, always consider the possibility that this person or situation may be a scam.

Scam Features – Phone callers

Scams often begin with a phone that is not recognizable. This may be and often is a clue that a scammer is on the phone.

1. In good business manners, **callers are supposed to identify themselves** with a first and last name. The use of a first name, or the fact that they do not know your name is already suspicious.
2. Know who you are dealing with. **Don't be afraid to ask questions**. Consider asking for their employee ID, the precise location of the business from which they are calling, and the address. If the caller resists attempts to get more information or acts pushy or angry, then the caller is a scammer.
3. If the person claims to be a business or is trying to sell you a product or service, **ask questions** and don't be afraid to take the time to research the business or products.
4. If the person claims he/she was referred to you by a friend, contact your friend to verify that it was really them that made the referral.
5. If a caller asks you for personal information, a credit card, social security number, date of birth, then it's a scam.

When Asked to Use Gift Cards

> No legitimate business asks for payments for merchandise or services in gift cards. Any entity on a call or by mail, or email, or text requesting or threatening and asking or demanding gift cards is a **scam.**

Scammers are getting smarter at using new technology to find ways to convince you to give them your money or personal information. But first, let's address keeping your computer and devices safe.

Shopping with Credit Cards

Many of us use credit cards or debit cards for shopping. It's convenient. There are federal laws providing some protections if a credit card is compromised. However, **there are no laws protecting the use of debit cards.**

If your card is a credit/debit card, always run it as a **credit.**

Never use a bank debit card for an online purchase. You are giving away too much personal information (like your account access). Consider having one card you always use for anything online. Then check it regularly to ensure nothing looks suspicious.

Financial Considerations

Senior Citizens often have a little nest egg tucked in a financial institution. Some investors elect to receive reports via mail, other by email. Some tips for protecting your money:

1. For viewing statements online, many institutions offer "two-factor identification." What this means is that after using a secure login and password, the system sends you verification to an email address or mobile phone number. When this is available, it is a good, recommended practice, even if it takes more time and is less convenient.
2. Anyone offering a "great financial deal" with promises of high returns – it is always possible the offer is a scam. Generally anything that sounds too good to be true is a scam. In the event it could be legitimate, take notes on the information and check it out with someone you trust, such as a banker or financial advisor.

Banking Scams

We interviewed Diane Porter from Bangor Savings Bank to learn the types of scams they are observing with their customers. Here is what was shared:

- You receive notification that you won something, inherited something (or variations) but there's just this fee you must pay up front for processing, or administration, or something similar.
- IRS Tax Overpayment Scam - Someone claiming to be from the IRS tells you by email or phone that you overpaid your taxes and they will process you a refund if only you provide your bank account number. **The IRS does not make phone calls**, unless returning your call.
- You sold something online on any popular site, and the buyer sends you a substantial amount of money *more* than the price (such as $1500 for something that cost $300). They claim they did

this in error, OR they are paying you extra for your inconvenience, and that you should pay yourself something for the inconvenience and send them (or wire them, or use moneygram, or Western Union, Etc.) the difference. The problem is that they don't want what you are selling, the check you receive is not a real check, but by the time you find that out, you may have already sent the difference (Your banker can trace a check to find out if it is legitimate).

- **Suspicious emails may arrive on your email or texts**; they may say your account is being charged, or you are getting a refund, or anything – But the crux here is that if you open the email or text, they are transferring malware onto your computer, tablet, or phone. This may be malware that **records keystrokes** and may be collecting all your passwords and bank account numbers each time you do banking or pay bills online.

Technology

Keeping your computer and devices safe

First of all, all computers need **anti-virus software**. This addition to your machine will scan regularly for threats. Vipre, Norton, and McAfee are common ones. They generally charge by the year and update regularly for software changes with no charge for the updates. NO computer is safe without a program for protection.

If internet service is via a wifi router (a black box with flashing lights and one or more antennae sticking up), your router has its own password. This differs from the password to access your computer, your email, or other things requiring passwords. If you don't know how to reset your router's password, your provider tech support line can assist. It is NOT acceptable to have the router password to be "admin." That's an invitation to hackers. NEVER use the word "password" as your password.

Scams on Your Phone, Tablet, or Computer

1. Do not open suspicious texts, pop-up windows or click on links or attachments in e-mails. Delete all of these. If in doubt, do an on-line search to determine whether the contact is legitimate.
2. Never give someone you do not know remote access to your computer. Scam callers will often ask you to turn on your computer to fix a problem or install a free upgrade, which is actually a virus that will give them your passwords and personal details.
3. Keep your mobile devices and computers secure by using password protections. Don't leave mobile devices unattended in public places. If you are in a restaurant and need to go to the restroom, take your device with you.

All About Passwords

Today there are more and more things for which a login and password are required. Consider making all your logins the same to avoid some confusion. Passwords are different, because the software which hacks passwords can only handle passwords up to 7 characters. **Make your passwords at least 10 characters long.**

To help you remember passwords, in addition to writing them down in an address book kept by the computer, consider a pattern by which you create your passwords. Consider putting together a grouping of:

1. One non-English word (something a dictionary program would not recognize).
2. Add numbers that mean something to you, but NOT your birthdate. Examples might be house numbers on places you used to live, birthdates of someone who has already passed away, or birthdates of a pet.
3. Decide on a non-word/number character to use, such as %,*, $, !. Most passwords require one.
4. Most passwords require one capital letter. Decide what may be capitalized, such as the first, last, or third letter of your word.

As an example, perhaps "Ziggy" is a good non-English word. Perhaps a childhood home's house number was 3456. Then consider a favorite non-word, non-number symbol, such as (!) or (&). These components can be assembled to one's liking and create a unique but personally meaningful password.

Ziggy!3456 or !3456ziggY or 3456Ziggy! It's important after deciding on a password to write it down. THEN, for each password, add something unique for the vendor. Such as Ziggy!3456CMP to access your electric bill. Or Ziggy!3456VER to access Verizon. Or, something unique can be added at the beginning, or middle, as long as it makes sense to the user.

Local Contractors

For the most part, local contractors are unregulated. Never engage a business that calls YOU. Only engage a business ***you*** **call**. If you are considering using any contractor for building, repairs, driveway paving, electrical work, yard work, new roof – anything – call around and get recommendations from people you know and trust.

Summary

Here's a summary of what was presented here. Save this for reference.

- Scammers are often foreign. Watch for mistakes in English grammar.
- Legitimate businesses never do business with gift cards.
- No government agency calls you to tell you anything concerning your money, debts, taxes, arrest warrants, social security, pension, etc. (unless they are returning your call). Everything is done by letter.
- Never give a bank account number, social security number, tax ID, birthdate, or anything else personal to someone who calls you.
- Anything that sounds too good to be true always is.

- If you sell online, do “local pickup only” so you are selling locally and meeting to complete transactions in a public place. No exceptions.
- Don’t click on anything on the phone, tablet, or computer that seems suspicious.
- When in doubt, call the fraud division of your bank, your pension company, your credit card company, or check in with local law enforcement.