NORA

CHAT SCAMS

Text and online messaging is a prime place for scammers to try and con you out of personal information.

We often make the mistake of believing that if someone has our number, we either should know them, or our number was given to them for a good reason.

Scammers take advantage of this assumption and have grown increasingly sophisticated about the way they exploit people. They will often pretend to be an acquaintance or a reputable institution like a bank.

- Verify the message via a different source
- If a friend, family member, bank or any other business ask you for personal information or money, validate the request by calling the company or person making the request.
- Beware of unknown or strange numbers
- Chances are, you already have a friend or family member stored in your phone under a familiar name.
- Notice poor grammar. If the text or chat is not using proper grammar, this is often a tip off that it's a bot or a scammer operating from a foreign locale.
- Don't respond. In the end, the safest response is no response at all. If the request is crucial the company or acquaintance will attempt to contact you in multiple different ways.

COMPUTER SCAMS

- If you spend any time online, you've probably been target of a phishing attack.
- This is when a scammer pretends to be from a reputable company in order to get you to reveal personal information they can use.
- Phishing is a technique that's often deployed through emails. Web site pop-ups, and even mobile apps.

General questions to ask yourself to avoid computer scams:

- Is this asking for too much information? Be wary of anyone who asks for more information than they need, even if you are talking to a company or bank you do business with.
- Do I know you? Ask this simple question before responding to a message. First check to see if you recognize the sender's name and email address.
- Is that a legitimate link? Before clicking on a link, hover over it to see if the URL address looks legitimate.
- Am I on the web page I think I'm on? Before logging into an online account, make sure the web address is correct. Phishers often forge legitimate websites, like online storage accounts, hoping to trick you into entering your login details.
- Is it too good to be true? Avoid "free" offers or deals that sound too good to be true.
- Is my security software active? Always use comprehensive security software to protect your devices and information from malware and other threats that might result from a phishing scam.

The CEO/Executive The scam appears as an email from a leader in your organisation, asking for highly sensitive information like company accounts, employee salaries, Social Security numbers, and client information.

File sharing & DocuSign Phony requests to access files in Dropbox and DocuSign accounts are on the rise, tricking workers into clicking on dangerous links.

The Romance Scam This one can happen completely online, over the phone, or in person once contact is established. But the romance scam always starts with someone supposedly looking for love. The scammer often puts a phony ad online, or poses as a friend-of-a-friend on social media and contacts you directly. But what starts as the promise of love or partnership, often leads to requests for money or pricey gifts. The lure here is simple-love and acceptance.

The Mobile Phish Scammers distribute fake mobile apps that gathers your personal information in the background or send text messages containing dangerous links

Surveys You get a request to take a survey for a social issue you may care about. When you click that link, you could be getting infected with malware.

The urgent email attachment Phishing emails try to trick you into downloading a dangerous attachment giving a bad actor access to your computer. Such emails ask you to download attachments confirming a package delivery, trip itinerary, or prize.

Phone scams come in many forms. Some act friendly while others try and use intimidation. In all cases, the goal is to get personal information and money.

How to protect yourself:

- **On changing or hiding telephone numbers:** While there is the Telephone Preference Service, this does not work with telephone calls outside the UK. There is a free reverse phone lookup website "Who called me?" which can give useful information as to (a) the location of the caller (not always accurate if the call is forwarded from outside the UK) but also comments from people who have answered or called back. There are also other similar sites such as "Unknown Phone Number".
- **Distinguishing between wanted and unwanted calls.** My own system is not to acknowledge or answer telephone calls which do not give contact details (which are on your contact list) and to block the number which is easy to do on mobiles.
- **Use call blocking** Your phone carrier may provide a service to block known phone spam numbers or at least ID them for you when your phone rings. Most of the major providers now offer a free service to reduce the number of nuisance calls: O2, BT, Sky, and TalkTalk, though Virgin Media offers a less sophisticated system.
- **Call Centres:** As above, once answered, these numbers can be blocked. The best way is just to hang up the telephone immediately. If you've got the time and inclination, and just to amuse yourself, try what I used to do when conservatory salesmen call. Let them go through all their patter and then ask the crucial question "how do you build a conservatory on a first floor flat?"!!! As the cartoon caption in "Punch" used to say "Collapse of Stout Party".

- **Telephone calls terminated by the recipient user:** Wait at least 10 minutes before using the phone or use another line if available. If Bank Details are requested, ***no Bank will ask you to give that information either by email or on the telephone***.
- **Banking frauds:** Large amounts should be transferred by direct communication with your Bank, either by letter or personal call (sometimes difficult if the local branch has closed). **The HMRC will never ask for details especially if there is an apparent "refund due" or a request for an underpayment of Income or other tax.**
- **Hang up**. Don't let them know they reached a responsive phone number. By pressing buttons or trying to talk to an operator, you may be in for even more robocalls.
- **Don't rely on caller ID as proof** Phone scams have become better at making you think it is a legitimate number by "spoofing" an ID and displaying some type of official name. Some even report it shows their own number calling them.
- **On changing or hiding telephone numbers:** While there is the Telephone Preference Service, this does not work with telephone calls outside the UK. There is a free reverse phone lookup website "Who called me?" which can give useful information as to (a) the location of the caller (not always accurate if the call is forwarded from outside the UK) but also comments from people who have answered or called back. There are also other similar sites such as "Unknown Phone Number".
- **Distinguishing between wanted and unwanted calls.** My own system is not to acknowledge or answer telephone calls which do not give contact details (which are on your contact list) and to block the number which is easy to do on mobiles.
- **Use call blocking** Your phone carrier may provide a service to block known phone spam numbers or at least ID them for you when your phone rings. Most of the major providers now offer a free service to reduce the number of nuisance calls: O2, BT, Sky, and TalkTalk, though Virgin Media offers a less sophisticated system.
- **Call Centres:** As above, once answered, these numbers can be blocked. The best way is just to hang up the telephone immediately. If you've got the time and inclination, and just to amuse yourself, try what I used to do when conservatory salesmen call. Let them go through all their patter and then ask the crucial question "how do you build a conservatory on a first floor flat?"!!! As the cartoon caption in "Punch" used to say "Collapse of Stout Party".
- **Telephone calls terminated by the recipient user:** ***Wait at least 10 minutes before using the phone or use another line if available.*** If Bank Details are requested, no Bank will ask you to give that information either by email or on the telephone.
- **Banking frauds:** Large amounts should be transferred by direct communication with your Bank, either by letter or personal call (sometimes difficult if the local branch has closed). The HMRC will never ask for details especially if there is an apparent "refund due" or a request for an underpayment of Income or other tax.
- **Hang up.** Don't let them know they reached a responsive phone number. By pressing buttons or trying to talk to an operator, you may be in for even more robocalls.
- **Don't rely on caller ID as proof** Phone scams have become better at making you think it is a legitimate number by "spoofing" an ID and displaying some type of official name. Some even report it shows their own number calling them.

:

Credit repair scams Give them some money and they promise to "fix" or "remove" your debt.

Charity scams You need to give money today to help these people in need.

Extended car warranties They access public purchase records to try and sell you overpriced or worthless car warranties.

Web Scams Scammers defraud many people using internet services and software. The goal of these scams is to trick you into sending money or personal information.

Avoiding web scams: Keep your computer software updated. Your operating system, web browsers and apps are constantly updating to adjust to the scammers' new tricks. This includes keeping your antivirus software subscription updated as well.

Buy from trusted sources. Do some research if you are not sure. Some antivirus software is a great resource for helping identify some unsafe sites when you attempt to visit them

Talk to your kids. Make sure they are educated on the dangers of online scams.

Fake commerce sites Fake product sites used to sell products that are not worth the price paid or not delivered at all.

Credit card fraud Asking for credit card information to proceed on a web site

Malware Software designed to disable your computer system for the scammers personal use or to simply damage it. Also, a general term used for viruses, spyware, worms, trojans, and more

Like many of these other scams, online scams exploit those in need or looking for a deal.

Look out for:

Prize scams You'll be notified that you just "won" a nice prize like money, jewellery or a vacation. These scams will ask you to pay something upfront. If a prize you won is too good to be true, it probably is. Do your research about the contest with a browser search. Many times, you will find stories of others that have already been taken.

Crowdfunding scams Creators of the crowdsourced request promise a return for your small investment in their project but end up pocketing the money instead. Never send money or gift cards to a person you have not met in person. Research any crowdfunding campaigns to see feedback from others and if they have not delivered on their promises. Always look for the **security lock** on sites asking for personal information

The most common email scams involve phishing. Phishing schemes take on the appearance of a legitimate email, they may even appear to be from a company you're familiar with, in order to exploit your trust and gain personal or financial information.

Types of email scams you may see

Foreign lottery scam You just won a big prize, often in a foreign country, but you must pay a small amount upfront to gain the larger reward

Survey scam You get a request to take a survey for a social issue you may care about. When you click the link, you get infected with malware.

Banking scam You receive an email saying there is something wrong with your bank or PayPal, Amazon, or other account that needs your attention. You're then directed to a fake site where you attempt to log-in so they can steal your user name and password for the actual site. Don't be tempted!

Acknowledgements to McAfee LiveSafe