HOW CAN I AVOID SPAM AND PHISHING SCAMS?

Knowing how to avoid scams, spam and phishing is a critical life skill. Fortunately, eleven simple safety measures will help you dodge the risks – whether the scam comes via the phone, regular mail, an email, or somewhere online.

Slow down.

Spammers want you to act first and think later. If the message conveys a sense of urgency, or uses high-pressure sales tactics be skeptical; never let their urgency influence your careful review.

Look for errors.

A great deal of spam is of poor quality with lots of spelling, grammar, and layout flaws. If you see obvious errors you know it's a fake. However, the lack of errors does NOT make the offer legitimate. Smart scammers can spell, and they can make a fake email look as good as a legitimate one.

Research the facts.

Never believe unsolicited messages offering financial solutions, hot stock tips, refinancing etc. If the email looks like it is from a company you use, do your research. Use a search engine or contact the company directly (see #6) to learn more. If the offer is for an investment, have someone at your bank, a financial consultant, or trusted advisor review the deal before handing over a dime.

Delete any request for financial information or passwords.

If you get asked to reply to a message by providing your bank account, bank routing information, credit card numbers or passwords, it's a scam.

Reject requests for help or offers of help.

Legitimate companies and organizations do not contact you to provide help. If you did not specifically request assistance from the sender, consider any offer to 'help' restore credit scores, refinance a home, etc. a scam. Similarly, if you receive a request for help from a charity or organization that you do not have a relationship with, delete it. Charity scams tug on heartstrings especially after a disaster strikes. To give, seek out reputable charitable organizations on your own to avoid falling for a scam, and research how much of the money donated will actually get to people in need.

Don't let a link in control of where you land.

Stay in control by finding the website yourself using a search engine to be sure you land where you intend to land. Hovering over links in email will show the actual URL at the bottom, but a good fake can still steer you wrong. Curiosity leads to careless clicking – if you don't know what the email is about, clicking links is a poor choice. Similarly, never use phone numbers from the email; it is easy for a scammer to pretend you're talking to a bank teller.

Beware of dangerous downloads.

If you don't know the sender personally AND expect a file from them, downloading is a mistake. Email hijacking, where spammers take over control of someone's email, has become rampant. Once they control someone's email account they send messages with malware to all of the person's contacts hoping to infect their machines.

Foreign offers are fake.

If you receive email from a foreign lottery or sweepstakes, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the money it is guaranteed to be a scam.

Scammers manipulate emotions.

If you're financially stressed, lonely, angry, sad, overly happy, frustrated, looking for romance, etc. you're more likely to fall for fraud. Put emotions aside when evaluating phone calls, mail, email, online offers, or notices.

Free has a price tag – and it's usually more than you bargained for.

Those offers to send you free trial products, or free anything, then say "you just pay shipping and handling" are scams. You'll pay more in fees than the product is worth. Even when you don't have to pay anything, the catch is that they are collecting all your information – you need to give your name, address, phone number, email address, and often more when signing up. This information will be sold and resold many times over.

Set your spam filters to high.

Every email program has spam filters. To find yours, look under your settings options, and set these high – just remember to check your spam folder periodically to see if legitimate email has been accidentally trapped there. You can also search for a step-by-step guide to setting your spam filters by searching on the name of your email provider plus the phrase 'spam filters'.