If It Sounds Too Good to Be True…

Somehow this email made it through your filtering system and flashes like a bright semaphore in your inbox:

"Congratulations! You are today's winner of a free iPad. Click here to claim your prize!"

Or how about this one?

"Get your free download of the world's most popular software. Click here to start."

Offers like these have been around almost as long as the commercial Internet. They comprise a vast and sometimes sleazy electronic flea market where scammers, questionable marketers, counterfeiters, and outright thieves compete for your attention. Today they have spread well beyond email to text messages, social media, pop-up advertisements, QR codes, and phone calls.

Fortunately, with a little practice and a healthy dose of skepticism, almost anyone can learn to recognize them.

People Cannot Afford to Give Expensive Stuff Away

Grandpa Walton on the 1970s television series *The Waltons* once told his disappointed grandchildren, who had received broken toys from a Depression-era charity giveaway, **"No one ever gave away anything worth keeping."**

That may be a little high on the cynicism scale, but it contains a useful lesson for navigating the Internet. Businesses may legitimately offer free samples, trial subscriptions, promotional gifts, or discounted products, but they normally expect something in return—your future business, your contact information, your attention, or your agreement to a subscription.

So when a stranger announces that you have suddenly won an expensive computer, phone, gift card, or pile of cash—especially when you never entered a contest—your first reaction should not be excitement.

It should be: **What does the person on the other end want from me?**

The Federal Trade Commission offers an especially simple rule: a legitimate prize does not require you to pay money to receive it. If someone demands "shipping," "processing fees," "taxes," gift cards, cryptocurrency, or some other payment before releasing your prize, there probably isn't a prize.

The Modern Bait-and-Switch

Years ago, clicking that free-iPad offer might have led you through a tedious obstacle course of registrations, surveys, coupon offers, trial subscriptions, and requests for personal information. After running that gauntlet, you might discover that the "free" iPad wasn't really free—or wasn't much of an iPad.

That kind of marketing still exists, but today's version can be considerably more dangerous. The link may take you to a convincing imitation of a legitimate company's website. You may be asked to enter an email address and password, a credit-card number, or banking information. In other cases, clicking a link or downloading a file may expose your computer or phone to malicious software.

The scammer doesn't necessarily want to sell you anything. **You—or your personal information—may be the product.**

That is why one of the best cybersecurity habits is also one of the simplest: **don't use the link in an unsolicited message to reach an important account.**

If a message supposedly comes from your bank, credit-card company, Apple, Microsoft, Amazon, or another company you do business with, open the company's app or type its familiar web address yourself. If there really is a problem with your account, you should be able to find it there.

"Free" Downloads Don't Necessarily Mean Free Software

Software offers require the same skepticism. Legitimate companies do offer free trials, free versions, and free downloads. Microsoft, Adobe, Apple, and other companies also allow software to be downloaded before a license or subscription is purchased.

The important distinction is between **free software** and a **free download**.

A website may truthfully allow you to download a program without charge, while the software itself requires a paid license or subscription before all its features will work.

More suspicious are websites offering activation codes or product keys for expensive commercial software at unbelievably low prices. Microsoft warns that independently sold product keys can be stolen, counterfeit, or otherwise unauthorized. A key may initially appear to work and later be blocked.

There is also a cybersecurity reason to stay away from questionable software sites. Pirated or modified software can contain malware, spyware, or other unwanted programs. Saving a few dollars isn't much of a bargain if you compromise the computer on which you keep your photographs, financial information, documents, and passwords.

For commercial software, the safest approach is straightforward: **download it from the developer or a reputable authorized seller.**

The Old Scams Haven't Disappeared—They've Improved

Remember those emails from some mysterious overseas official who needed your help transferring $50 million? They're still around in various forms, but today's scams can be much more convincing.

A message may claim that your bank account has been compromised and urge you to “verify” your identity immediately. Another may say that a package cannot be delivered until you pay a small fee. A text might warn you about an unpaid toll. A caller may pretend to represent Microsoft, Apple, your bank, the government, or even a family member in trouble.

Scammers increasingly use information gathered from social media and other sources to make their stories more believable. Artificial intelligence can make fraudulent messages more polished and can even help criminals imitate voices and images. The awkward spelling and strange grammar that once helped identify scam messages can no longer be counted on as reliable warning signs.

The basic strategy, however, hasn't changed. The scammer wants you to react **before you think**.

Watch for Pressure

Urgency is one of the scammer's most effective weapons:

- **Act now.**
- **Your account will be closed.**

- **Your computer has been infected.**
- **Your package cannot be delivered.**
- **Your grandson is in trouble.**
- **This offer expires in ten minutes.**

A legitimate business problem will usually survive the few minutes it takes you to investigate it independently. Stop. Don't click the link. Don't call the telephone number supplied in the suspicious message. Don't provide a verification code that suddenly appears on your phone.

Instead, contact the company or person through a telephone number, app, website, or contact information you already know to be legitimate.

Beware of Strange Ways to Pay

How someone wants to be paid can be an enormous warning sign.

Be especially suspicious when someone unexpectedly insists on payment by gift card, cryptocurrency, wire transfer, bank transfer, or a payment app—particularly when you're being pressured to act immediately. These payment methods can make recovering stolen money difficult.

And nobody from the government, your bank, Microsoft, Apple, or a legitimate business is going to tell you to buy gift cards and read the numbers from the back to settle an emergency.

Your Best Scam Detector Is Still You

Spam filters, antivirus programs, browser protections, and security software are much better than they were when these scams first appeared. But no filtering system catches everything.

That's where you come in.

Treat unsolicited messages involving money, prizes, passwords, account problems, investments, jobs, or emergencies with suspicion. Don't provide personal or financial information simply because someone asks for it. Don't allow a stranger who unexpectedly calls you to take remote control of your computer. And don't assume that a familiar company logo, caller ID, email address, or professional-looking website proves that the person contacting you is legitimate.

Most importantly, remember that scammers depend upon two very human emotions: **fear and greed**. One says, *“Something terrible will happen if I don't act immediately.”* The other says, *“I can't pass up this opportunity.”*

When either one starts talking, give your common sense a chance to answer.

Grandpa Walton's advice may have been overly pessimistic. There really are worthwhile things that are free.

But that unexpected free iPad?

Don't click on it.