While good antispam software will prevent most spam from reaching your inbox, it’s not perfect. In the world of cybersecurity, it’s foolish to think you are 100% safe. Doing so makes you more vulnerable and more likely to be the next victim. Often with cyberattacks, pride comes before the fall.

Just as your municipality may have the best police officers serving your community, they cannot guarantee 100% that a bad guy won’t drive into your community today. Now, multiply that situation many times over with the internet. A cybercriminal can be working alongside you (yes, in your office), in your city or village, in your county, in your state, somewhere in the country, or across the globe.

We need to stay vigilant, keeping a careful watch for the possible dangers. With spam, some emails will still come through that attempt to trick you. Here are five that you must be extra careful about.

**FEAR-BASED EMAILS THAT SEEM LIKE THEY ARE LEGITIMATE**

These kinds of emails come in many flavors, but all have the same theme. For example:

- **Banks and financial institutions** “alerting” you: You receive an email from your bank that tells you something froze your account and you need to click a link to “confirm your credentials” and log back in.
- **Government agency threatening you**: The IRS, FBI, or some other government agency threatens you with legal action or financial penalties unless you log in to correct an error.
- **Retail stores and online brands luring you in**: Emails from Apple, Best Buy, or Netflix tell you about a big discount, sale, or error with your account - requiring you to log in.
- **Software or applications warning you**: You receive emails from Microsoft, Google, or Facebook telling you about some technical error and that you need to log in to fix it.

Glaring red flags exist (such as the sender’s email address and grammatical errors), but these emails are improving over time to look and sound like banks and other trusted institutions. If you are a Chase customer, then you might glance at this quickly and click.

Always be skeptical of these “legitimate” emails, especially if they seem to be scaring or threatening you. If you have any doubt, call the company directly about the issue.

**EMAILS FROM “TRUSTED” SENDERS**

These can be very, very tricky. Here are two real examples:

### From: Nathan Eisner <admin@ocess.net>

Sent: Tuesday, October 02, 2018 10:57 AM

To: [OMITTED FOR EXAMPLE]

Subject: Direct Deposit Info Update

Sue,

I changed my bank and I’ll like to change my paycheck dd details, can the change be effective for the current pay date?

Regards

Nathan
In both cases, it looks like the email comes from a trusted contact. In Paris’s case, the spammer was sophisticated enough to even spoof the city manager’s email address. But note three big red flags:

- A request for unusual information.
- A tone that doesn’t quite match the tone of the trusted contact.
- Odd grammatical errors.

If you have the slightest doubt or something seems odd about an email from someone you trust, call the sender directly and ask if they actually sent you that email.

**TRICKS TO GET YOU TO CLICK**

Many spammers try to use tricks to get you to click that include:

- **Delivery Failed:** When emails bounce, you typically get a notification but you’re not required to do anything. But when you get an email message - sometimes out of the blue, even if you haven’t sent emails recently - that tells you several messages were not delivered, you should never click on it to “find out more.” That’s not how email works.

- **You Have Unread Messages:** Don’t ever fall for an email that says “you have unread messages” and requires you to click on it. Do you know how you should find out if you have unread messages? Look at the ones in your inbox that you haven’t read. Most email software clearly shows you what’s read and unread, and there are options that help you filter unread from read email messages.

- **“Re:” Messages:** If you see a message with “Re:” in the subject line, you might think it’s part of an earlier conversation - and thus you’re more likely to think it’s valid. However, many spammers insert the “Re:” into emails to trick you into thinking you’re responding to an ongoing email thread.

Here’s an example of the “delivery failed” email, with plenty of red flags (sender’s email address, unusual message, call-to-action that's not the usual way to work with email, etc.).

**UNKNOWN OR UNTRUSTED VENDORS**

This falls into a gray area. Many vendors, of course, still buy email lists and blast out emails across a wide variety of industries. A modern spamming tactic - which sometimes involves shady or less reputable vendors - is to reach out to “prospects” in a normal business way. Then, if you click and get interested in doing business with them, you may get promised something that the company won’t deliver.

For example, it’s clear that this email raises a few red and yellow flags:

While this certainly may be a legitimate business, here is why you need to be suspicious.

- The company’s name is never mentioned.
- A link to the company’s website is not provided.
- No basic contact information (address, phone number, etc.) is provided.
- The sender’s email address is generic, rather than including the domain name of the supposed company.
- It says “Hey” without mentioning the person’s name receiving the email, which is unprofessional and suggests this is a mass email without personalization.
- It’s unsolicited.
- This person cannot be found on LinkedIn.
- Searching for “rekha tiwari custom web designing” on Google turns up nothing.
If this isn't a scam, then the business is doing all the wrong things to market itself. Either way, stay away!

**UNSOULICITED ADS**

Again, this can possibly be another gray area. However, it's a good general rule of thumb to avoid unsolicited ads from companies that are untrusted and not within your known network.

Here's an example:

On the surface, it looks legitimate -- including a reasonable offer and a corporate address. And yes, Terminix is a legitimate $1.45 billion company headquartered in Memphis.

However, look at the sender's email. The “amplespar.click” domain does not look legitimate. Also, the email requires you to download pictures to get the content. While many legitimate newsletters do require you to download pictures, usually you can read some text without having to do any downloading. In this case, so little information about this offer is included that, with the suspicious email to add to the clues, it’s clear you should pass on it. (Plus, after opening this type of spam email simply to look at it, it's not uncommon to receive another email within minutes from them with a different “offer”).

Even if the offer is legitimate, only engage with these emails if you absolutely know you subscribed to them and you're used to a consistent look and feel. Pause to consider if this is an email you would expect to receive, or one you have received in the past. Is it reasonable that you should get this email? And even then, be careful. (Many companies will also share product and service promotions directly with you on their websites or in their stores).

While employee training and awareness helps you spot these tricky emails, remember to supplement your efforts with good enterprise-level antispam software that:

- Stops most spam before it gets to your inbox.
- Sends the remainder of this spam to your junk mail.
- Allows you to set strict filters so that you can go through your junk mail and whitelist trusted senders.

**FINALLY, HERE ARE 5 TIPS ON HOW TO SPOT PHISHING ATTACKS THAT TAKE ONLY SECONDS**

1. **Review every letter in the sender's email address.** I want to stress “every letter.” Don’t quickly glance at the sender's email address because it's too easy to miss one letter being different - and cyber criminals know we are too trusting and busy! Is this an email address from one of my contacts? Does the email address look legitimate or one from whom I expect to receive email? Does the sender's email address change if I reply to the email? If answering these questions causes you any doubts, then these are red flags.

2. **Never click a link or download an attached document unless you are 100% (not even 99.99999%) sure it is legitimate.** You must be 100% sure that the email is legitimate before clicking or downloading.

3. **Ask yourself, “Am I expecting this email?”** Is it reasonable that you should get this email?

4. **Hover over the links.** Know that emails can include very long URLs that get translated into shorter URLs after you click. This is part of how email programs work. However, if you have doubts about an email (especially if you're receiving an email from an organization for the first time), hover over the links with your cursor (but don’t click them). At the bottom of your screen, you will see the URL appear. Look at these URLs to see if you identify the name of the organization that sent the email (such as sophicity.com). If the URL looks very different from the sender's organization (especially if it doesn't even mention the organization's name), then it may be spam. Remember, URLs can also be spoofed, so if you have any doubts at all, use the additional tips in this article to examine other aspects of the email that assess its trust factor. If you're not 100% sure, contact your IT support and have them review it.

5. **If you are not 100% sure about an email, get a second set of eyes on it.** Ask someone you trust. Hopefully your IT support will review it, but you can also get someone next to you in the office to look over your shoulder at the email and take a look. And don’t worry - checking emails like this is not the norm. It will be an exception that you will have to ask someone to review an email, if you follow the steps above. However, in these exceptional cases it's much better to take a few seconds to do this rather than take hours, days, weeks, or months cleaning up a mess from a cyber incident.

When you know the email is a risk, don't just delete it. Mark the email as spam or junk (depending on your email software) so that others too can benefit from your good work at spotting phishing.