Summer Scams

These days, online scams come in a host of guises, making it hard to identify them as scams. But the end game is always the same: the bad guys are looking to steal your personal information for their own financial gain or to infect your computing devices.

Most scams fall under the umbrella of social engineering—the art of human manipulation to gain trust. If a cyber criminal can gain your trust, he or she can lead you to break your normal security procedures by divulging information and unknowingly downloading a malware-laden attachment or following a phony link.

Here are the top three scams we've seen most recently:

1) The Microsoft scam

Potential victims of this scam receive a call from someone claiming to be a Microsoft technology specialist or a tech from another well-known company. The caller explains that he or she has detected viruses on the targeted computer. Unless the "tech" is allowed to fix the computer immediately for a fee, viruses will render it unusable.

The person on the other end of the line is, of course, a hacker aiming to con the potential victim out of money and gain remote access to the user's computer. The access could last even after the phone call ends, enabling the hacker to track the computer's daily activity and steal sensitive information over a period of time.

Microsoft and other well-known technology companies *do not* call users of their products to notify them that there's something wrong with software or hardware. So if you receive a call from a supposed techie, hang up! (If you are actually experiencing a problem with your computer, by all means call Microsoft Support yourself or another reputable and trusted IT entity, like Geek Squad.)

2) The Google Drive/Dropbox file-share scam

With this scam, recipients get an e-mail claiming that they have a very important document ready to view on Google Drive or Dropbox. When the recipient clicks on a link provided, he or she is taken to a fake website that looks almost identical to the legitimate Google login or Dropbox website. Of course, what's really happening is that the recipient is turning his or her login credentials over to the hacker and potentially downloading malware.

If you receive a request like this from an unfamiliar e-mail address, **don't click on the link** and be sure to delete the e-mail. If you receive a request from a known entity, reach out to determine whether the request is legitimate, or go to Dropbox or Google directly from your browser to log in.

3) Fax report and wire transfer scams

Lately, we've seen many phishing e-mails claiming that recipients have a **fax report** ready to view and that they should click a link provided to access it. The link leads to a bogus website with the ability to infect the recipient's computer or device with malware.

The **wire transfer** scam e-mails come in various forms. A recipient may be alerted that a recent wire transfer was canceled or aborted by his or her bank. Or the e-mail may say that the sender recently received a wire transfer request from the recipient and needs confirmation before proceeding. To view the details, the recipient has to follow a link or download an attachment, resulting in exposure to malware.

If you receive e-mails like these, **don't click on any links or attachments** and be sure to delete the e-mail. If you are indeed expecting a fax or have recently initiated a transfer request, call the organization that purportedly sent the e-mail *at a known phone number*.

Stay aware

Remember, if you get a call from a tech claiming that he or she needs to clean up your device due to viruses, hang up and contact Microsoft, Apple, or your trusted IT professional directly. The same thing goes for unsolicited e-mails:

visit the organization’s website by typing the known URL directly into the browser yourself or simply call the company or individual.