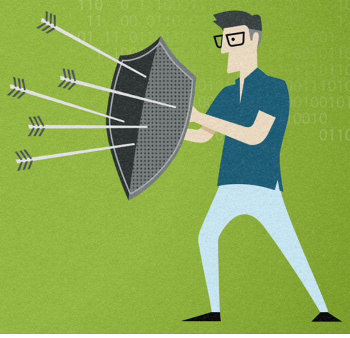
Five ways to detect a malicious ‘phishing’ email



At least since the time email first started gaining widespread popularity in the 1990s, phishing scams have been showing up in email accounts. They’re called “phishing” emails because the cybercriminals who send them are fishing for victims.

These fraudulent emails, which may appear to come from a legitimate company or even a personal acquaintance, are designed to trick people into giving up personal information, such as credit card and social security numbers. They may also be designed to scam unwitting victims into opening a harmful attachment or clicking a link that unleashes ransomware or some other type of malicious computer virus.

Back in the early days of the internet, phishing emails were full of typos, and laden with obvious clues—appeals from faraway princes or rich relatives you never knew you had. These were very easy to spot. But cybercriminals have upped their game since then. For example, some cybercriminals go to great lengths to match the branding, color schemes and logos associated with the companies they are trying to impersonate.

Phishing email scams generally fall into one of these categories:

Traditional phishing attack

The traditional phishing attack casts a wide net and attempts to trick as many people as possible. A classic example of this is the Nigerian prince advance-fee scam.

Spear phishing

Spear phishing attacks are designed to target a specific individual or small group of individuals. For example, a spear phishing attack may use information about a particular restaurant or small business to target one or more employees at that business. Or it could look like an email from a friend.

Whaling

Whaling attacks, which have become increasingly popular in recent years, are targeted at high-profile victims like C-level executives and their teams. A typical whaling email may look like it was sent from the CEO of your company. But it’s really a fake designed to get you to share valuable information about the company.

Five ways to detect a malicious ‘phishing’ email

Protect yourself from phishing scams

Phishing emails may be more difficult to identify these days, but there are some important steps you can take to avoid becoming a victim. If you answer “yes” to any of the questions below, there’s a very good chance that you’re looking at a phishing email.

1. Does the message ask for personal information?

Always remember that reputable businesses do not ask for personal information—such as social security and credit card numbers—via email.

2. Does the offer seem too good to be real?

If it seems too good to be true, it’s a fake. Beware of emails offering big rewards—vacations, cash prizes, etc.—for little effort.

3. Does the salutation look odd?

Reputable companies will use your name in the salutation—as opposed to “valued customer” or “to whom it may concern.”

4. Does the email have mismatched URLs?

If you receive an email from an organization that includes an HTML link in it, hover your mouse over the link without clicking and you should see the full URL appear. If the URL does not include the organization’s exact name, or if it looks suspicious in any other way, delete it because it’s probably a phishing email. Also, you should only visit websites that begin with “https” because the “s” at the end indicates advanced security measures. Websites that begin with “http” are not as secure.

5. Does it give you a suspicious feeling?

Trust your instincts when it comes to email. If you catch yourself wondering whether it’s legitimate, and your instinct is to ignore and delete it—then pay attention to that gut check.

As email scams become more sophisticated, it is more likely that an employee at your company will fall victim to a phishing technique. Having a solid backup strategy will ensure you’re able to quickly recover from any instance of employee error.

Learn more about Carbonite data protection today.

Visit Carbonite.com.