# Keep Your Employees from Falling for Email Scams

While email phishing scams arrive in our personal email frequently, they also appear in our work email boxes and texts.

Be sure to talk to your employees about possible spam at work. While they may be suspicious about scams on their personal phones and computers, they may let their guard down while using company devices and make poor decisions. Then, opening potentially harmful spam emails becomes a *company* problem.

Remind your employees to scrutinize all unexpected emails as they may be disguised as company-related issues like:

- a problem with their account
- healthcare plan changes
- suspicious log-in attempts
- online registrations
- overdue invoices or payments
- software updates

Email scams aren't always easy to spot. These cyber crooks are pretty good at what they do. The email may even appear to come from *you*. Here are some red flags for them to watch for in their messages:

- Suspicious sender addresses or urls
- Typos, poor grammar, poor quality logos
- Questionable web links, buttons, or attachments
- Urgent request for information or action

Advise everyone to notify you if they receive a questionable email so you can review it for authenticity. Then you can make that decision.

The Federal Trade Commission has a good post about recognizing phishing, How to Recognize and Avoid Phishing Scams, that you can review.