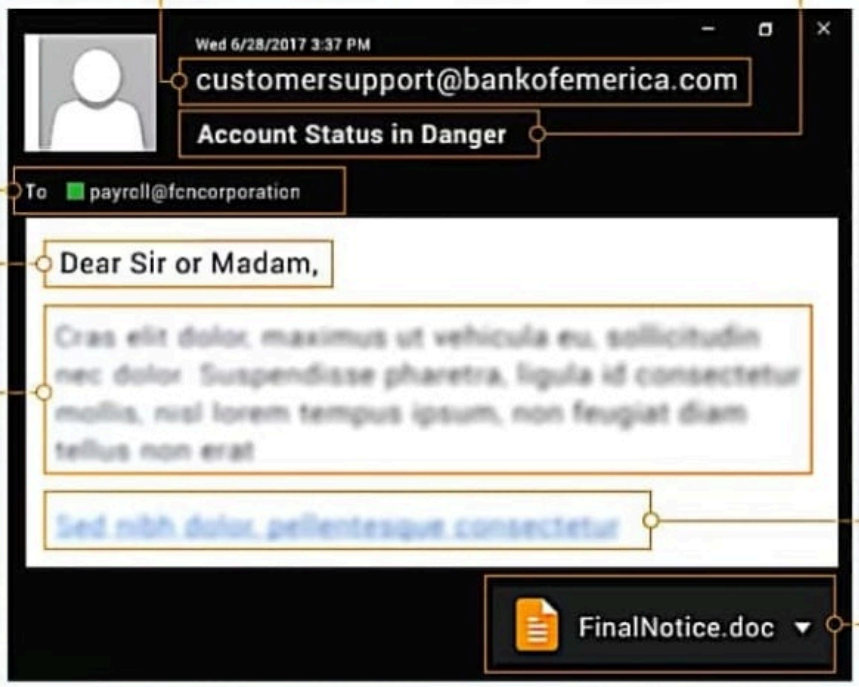
HOW TO SPOT A PHISHY EMAIL

Keep an eye out for misspellings, such as legitimate business names that are missing or off by just one or two letters. Additionally, an unexpected email from an address you've never communicated with before is a good early sign of a possible scam.

Subject lines containing too-good-to-be true offers or threatening statements meant to elicit an emotional reaction are clues someone's trying to phish you.

Watch out for mass email sends or unexpected emails to email aliases, like payroll@companyxyz.



Extreme caution should be exercised with any link appearing in an unexpected or unsolicited email. Hover over hyperlink text (or long-press on mobile) to see where the URL would actually direct you if clicked. Scammers will also try to implant real business names in fake URLs, so be wary.

Any messages addressed generically, especially ones regarding financial transactions, are suspicious.

Phishing email text can take many forms, whether it's threatening legal action or telling you an unexpected package has arrived. In general, be on the lookout for:

- Demands to click
- Unreasonable free offers
- Bad grammar or misspelled words

In all circumstances: **unexpected attachments should not be opened.** Many email systems will flag or altogether block attachments for this reason. But when they don't, it's all up to the person receiving the file to decide what to do.

The You Factor

The signs above are good overall points to look for when scrutinizing a suspicious email.

However, they do not represent all the ways in which scammers will attempt to phish you or your employees. That's why a separate but vitally important way of spotting a phishing email should be pointed out. And it's sitting right where you are.

That's right, it's *you*.

You have the best understanding of what sort of emails you usually get at home and at work. If an email just *feels* off for any reason, that's enough to be wary of it.

The sheer ingenuity of cybercriminals almost guarantees the coming years will bring phishing attempts no one has ever seen before. That's why a healthy dose of security awareness, with some skepticism and situational awareness thrown in, can go a long way.