How to Identify a Smishing Attack

AN UNEXPECTED SCARY MESSAGE

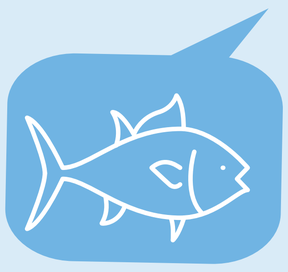
Sometimes, a hacker will try to scare you into clicking an infected link. They might say your bank account's been compromised or that you have minutes left to change a password. If you get a message like this, always question it—hesitating might just save you from being Smished.

A NUMBER YOU DON'T KNOW

We've all been taught to be suspicious of strangers, and strange numbers are just an extension of that. If you don't recognize a number that's texting you, be cautious. It's possible the texter's not who they claim to be.

RIDICULOUS TEXT

Not all hackers are sophisticated. Some might send a text that has nothing to do with you or that sounds too general to be legitimate. If the text sounds fishy… it's probably smishy.



POOR GRAMMAR

If the person texting you can't even spell your name right, chances are you don't actually know them. Weird punctuation, capitalization, and syntax are all warning signs of a Smishing attack.

IDENTITY CRISIS

Does the person texting you sound… off? Kind of like they're not themselves? If that's the case, there's a plausible reason: maybe they're not themselves at all!

ONEPATH