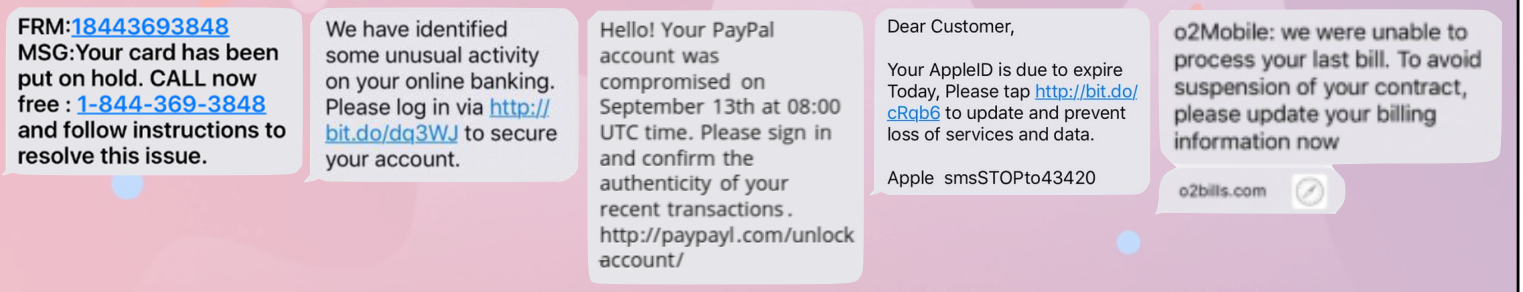
Whether you use an **Android** or **Apple smartphone or tablet,** crooks can easily send you **text messages** that look **urgent and legit.**

A text arrives from your bank: *oh no, you're overdrawn and your account is frozen!* Or the text says *you've won something cool!* Or a text from a friend or family member urges you to *check out this amazing new video!*

These texts, which are called "*smishes*," can be quite convincing. **More than 90% get opened.**

Here's what fake text messages look like.



Here's what crooks are after.

Because you're usually busy when using your phone and because you're less likely to suspect a text message is risky, fraudsters have found success ripping off unsuspecting users this way.

They want information about your bank account, social security number and zip code. They may convince you to install an app that looks useful but actually records and sends back every word you type.

Signs your device is infected include pop up ads that appear as you surf the web and apps that quit unexpectedly. Your phone may run hotter than usual and your monthly cell phone bill may be unexpectedly high.

Here's how to protect yourself.

Don't reply at all. Don't return the call, click on the link or respond by texting "STOP."

Avoid using public Wi-fi. Instead, use your own hotspot or link the device to your smartphone.

Keep your operating system up to date. When notified that an update is available, install it right away.

If you think you've responded to a smishing text, immediately change the password for the account that's involved.

SYNOVUS®