

9/28/15

From the Council of Better Business Bureaus

Scammers are always taking advantage of what's new and popular. This time it's WhatsApp, a smart phone application that allows users to send text, video and audio messages via the Internet. Scammers are impersonating the app to spread malware.

How the Scam Works:

You receive an email that appears to be from WhatsApp. The subject line reads "Incoming Voice Message" and a time stamp. Open up the message, and you'll see a "missed voicemail" alert and a button to play the message.

The email uses WhatsApp' colors and logo, so it looks legitimate. But don't click to play! WhatsApp says it does not communicate with customers via email unless they are replying to a specific customer request. The email is really a trick to download malware to your device.

This is far from the only scam pretending to be WhatsApp. Also look out for messages enticing you to click on links or download attachments. These scams typically claim that your account is being suspended or you are eligible for a new service.

Tips to Protect Yourself From a App Scam

Scammers love to impersonate popular apps. Here's how to spot a con:

- **Get antivirus software for your phone.** Just as you use antivirus software for your computer, you should get similar software for your mobile devices.

- **Know how a service communicates with you.** Most apps communicate with you through the app, offering updates, bug fixes, etc. If an app suddenly communicates using a different channel, that's a red flag. Be wary of any change from the norm.
- **Search before you click.** If something seems suspicious, do a quick search online. You can easily find out if the new deal or feature is for real.
- **Watch for the usual warning signs.** Scammers might be impersonating the latest tech companies, but that doesn't mean their scams are sophisticated. Look for poor grammar and reply email addresses that don't match the business.
- **Verify -- but not by using a source scammers give you.** Check if an offer is real, but don't call the phone number or website in the email you suspect may be a scam. If it is a con, chances are the person on the other line will be involved, too.

For More Information

To find out more about other scams, check out BBB Scam Stopper (bbb.org/scam). Learn more about scams pretending to be [WhatsApp on their website](#).

NOTE: WhatsApp is owned by Facebook, a BBB Accredited Business.

This Scam Alert has been sponsored by Western Union, a BBB National Partner.