There are two things guaranteed during and after Prime Day events: sales on Alexa and Kindles, and an increase in scams. The USPS is warning people of a rise in "smishing" scams. Delivered as text and SMS messages, the scams trick people into clicking on a link to steal login information. I'll show you what they look like, what happens if you click one, and what you should do instead.

TRT 134
STD OUT

SUPER
0-8 Jamey Tucker/whatthetech.tv

ON-CAMERA TEASE:

if people do online shopping, scammers are doing online smishing. I'm Jamey Tucker coming up with a term you need to know for a scam you'll probably receive.

ANCHOR INTRO

THE U.S. POSTAL SERVICE IS WARNING PEOPLE ABOUT A RISE IN A PARTICULAR TYPE OF SCAM THAT YOU MIGHT RECEIVE IN A TEXT MESSAGE AND THE NUMBER OF VICTIMS ALWAYS GOES UP AROUND THIS TIME OF YEAR.

IT'S CALLED "SMISHING SCAMS" AND CAN BE QUITE DANGEROUS. OUR CONSUMER TECHNOLOGY REPORTER JAMEY TUCKER HAS MORE ON WHAT TO WATCH FOR.

PACKAGE SCRIPT

Smishing scams are like clockwork this time of year. That's because lots of people are waiting on items they've ordered And in the last few years, smishing incidents have risen dramatically.

Smishing is a combination of SMS, as in texts, and phishing. Those scams that try to trick you into sharing information.

You've probably already seen one, like this. It looks legit, notifying me that a package I ordered can not be delivered. It even has "USPS" in the address. It urges me to reply Yes, or Y, to confirm my address in order to receive my package that's stuck in a warehouse somewhere.

If you reply with "yes", you'll get another text with a link. Two things can happen if you click it. It might ask for personal information or to log into your Amazon account. It might even look exactly like the Amazon login page. Or, maybe worse, a click could install malware on your phone, steal data on the phone, or even hijack your account. Pretty nasty stuff.

You should delete the smishing text, but before you do, forward it to the FCC, by simply holding down the message, tapping "More" and forwarding it to SPAM. Then, report it to your carrier by marking it as junk.

If you're expecting a package, go to your account page where you ordered it from to see if there's a delay. And tell your younger family members too, another report shows most millennials are unfamiliar with smishing scams.

That's What the Tech? I'm Jamey Tucker

ANCHOR TAG

THE LATEST DATA SHOWS OVER 240-THOUSAND PEOPLE FELL VICTIM TO SMISHING SCAMS IN 2020, COSTING THEM OVER 54 MILLION DOLLARS.

WEB STORY

Smishing scams are like clockwork this time of year. That's because lots of people are waiting on items they've ordered on Amazon Prime Day, and sales events at Walmart, Best Buy, and Target. And in the last few years, smishing incidents have more than doubled. The FBI's cybercrime complaint division said that in 2020, over 240,000 people lost a combined $54 million due to smishing, and phishing scams.

Smishing is a combination of SMS, as in texts, and phishing, those scams that try to trick you into sharing information in an email.

You've probably already seen one come through your inbox. They look legit, notifying the victim that a package they've ordered can not be delivered. It might even have "USPS", "UPS", "FedEx", or "Amazon" in the message or address. A smishing text will usually either ask you to respond with a "yes", or include a link to confirm your location.

If you reply with "yes", you'll get another text with a link. Two things can happen if you click it. It might ask for personal information or lead you to log into your Amazon or other account. It might even look exactly like the Amazon login page. Or, maybe worse, a click could install malware on your phone, steal data on the phone, or even hijack your account. Pretty nasty stuff.

This can happen even on an iPhone. Recent updates from Apple have been to patch zero-day security vulnerabilities, meaning hackers were already using the vulnerabilities to hack into iPhones.

You should delete the smishing text, but before you do, forward it to the FCC, by simply holding down the message, tapping "More" and forward to "SPAM", then report it to your carrier by marking it as junk.

If you're expecting a package, go to your account page where you ordered it from to see if there's a delay. And tell your kids too, another report shows most millennials are unfamiliar with the term "smishing".