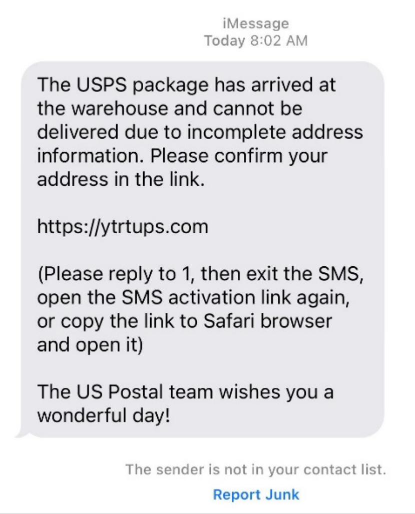
SUMMER 2023 E-NEWSLETTER

At Digital Mountain, we assist our clients with their electronic discovery, digital forensics, cybersecurity, and data analytics needs. For this E-Newsletter, we discuss mobile device messaging risks to organizations, as well as legal and data security implications.

Battling Phishing and Smishing with Tech Tools

Smishing and Phishing are annoying, but more than that, they're dangerous. These attacks can install malware on networks and mobile devices, steal login credentials, and ultimately lead to the exposure of PII/PHI. One reason phishing and smishing works is that, as social engineering attacks, threat actors are adept at creating realistic, often urgent-sounding messaging. Let's look at the following screenshot of a real smishing text recently received:



iMessage
Today 8:02 AM

The USPS package has arrived at the warehouse and cannot be delivered due to incomplete address information. Please confirm your address in the link.

https://ytrtups.com

(Please reply to 1, then exit the SMS, open the SMS activation link again, or copy the link to Safari browser and open it)

The US Postal team wishes you a wonderful day!

The sender is not in your contact list.

Because we all want our packages delivered correctly, we can understand how tempting it would be for someone to want to copy and paste that link into a browser and make sure the delivery address is correct. However, if we take a closer look, that link isn't directing to USPS.com, the US Postal Service's website. Additionally, as close to grammatically correct as the message is, some of the details should still raise questions. For instance, there's no information about the sender of the package, there's no USPS tracking number for the package, the instructions to activate the link are confusing, and finally, the "US Postal team" is an inaccuracy – the United States Postal Service consistently uses USPS, US Postal Service, or the Postal Service. While taking a second to evaluate a text from an unknown source is always the smart first move, relying solely on our scam detection skills isn’t going to bring an end to smishing texts. We need to do everything we can to fight threat actors on the mobile front.

Working Backward from Do Not Call

Thanks to telemarketers of all types, we know we should list all our telephone numbers, landline and mobile, on the FCC’s Do Not Call registry. That consumer protection database is distributed to carriers, and they are supposed to ensure that they are preventing those registered numbers from being programmed into automated dialing databases. While there are legitimate exceptions like a school district calling parents to inform them of a school closing, we also know that threat actors do not abide by the rules and will call or text as they please. Perhaps as an acknowledgement of the incomplete protection provided by the Do Not Call registry, the FCC developed the Do Not Originate list (“DNO”). The DNO list is a database sent out to carriers alerting them to numbers being used by rogue telemarketers and scammers, and therefore, calls originating from those numbers should not be allowed through the distribution network to end-user phones. If a legitimate user’s number is placed on the DNO list, the subscriber has the ability to request whitelisting. Again, not perfect, but a step up from the Do Not Call list by itself, and several steps up from cursing at random calls.

Update and Delete Frequently

Mobile device operating system and app developers have a vested interest in keeping threat actors at bay. First, the reputation boost that a developer or mobile device manufacturer gets from being security conscious goes a long way to securing market share. Protected customers are loyal customers. Second, the threat of an attack that leads to the discovery of an unknown vulnerability which in turn explodes into a cybersecurity event keeps developers up at night. In this case, the ounce of prevention needed is making sure that mobile device operating systems and mobile apps are updated to their most recent versions. Bug fixes, patches, and vulnerability hardening can be the invisible protections that prevent a mistaken or hasty click on a smished link from becoming a serious problem.

Conversely, deleting apps you don’t use often, cleaning out contacts, and not overloading your phone with all the latest games can also help prevent a smish from turning into a disaster. Threat actors have been known to use apps other than iMessage and Google Messages to send smishing texts with fake update notifications. These notifications include a link to a site that can ask for (steal) login credentials, scrape data, including contacts, and install malware and keystroke logging code. Your best bet? Get rid of any apps you don’t use regularly, download only necessary apps from trusted developers, and use your device’s native updating service instead of clicking on urgent update notification texts.

Honestly though, there’s one strategy that we can never emphasize enough: training people to recognize the warning signs of and the proper response to phishing and smishing attacks. Like soldiers on the front lines, individuals can do more to bring about victory in the war against threat actors than they probably realize. A social engineering attack, like phishing or smishing, relies upon a connection to someone on the other end of the transmission; and as such, their vigilance is crucial to this fight. Engaging with cybersecurity professionals to conduct vulnerability assessments and penetration testing is just the first step in an organization’s comprehensive approach. The most important step will always be having cybersecurity professionals work directly with the entire organization to ensure that each member of the organization is ready to take on their important role in the battle to stop phishing and smishing. At Digital Mountain, we're here to assist with tabletop exercises, training, and other cybersecurity needs.

Please direct questions and inquiries about electronic discovery, digital forensics, cybersecurity, and data analytics to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

DFRWS USA 2023
Baltimore, MD: July 9-12, 2023

MASTER'S CONFERENCE JULY 2023
Seattle, WA: July 19, 2023

PFIC 2023 VIRTUAL
August 1-4, 2023

ABA2023 ANNUAL MEETING
Denver, CO: August 2-8, 2023

SANS DFIR SUMMIT
Austin, TX: August 3-4, 2023

Click here to see more upcoming events and links.

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: