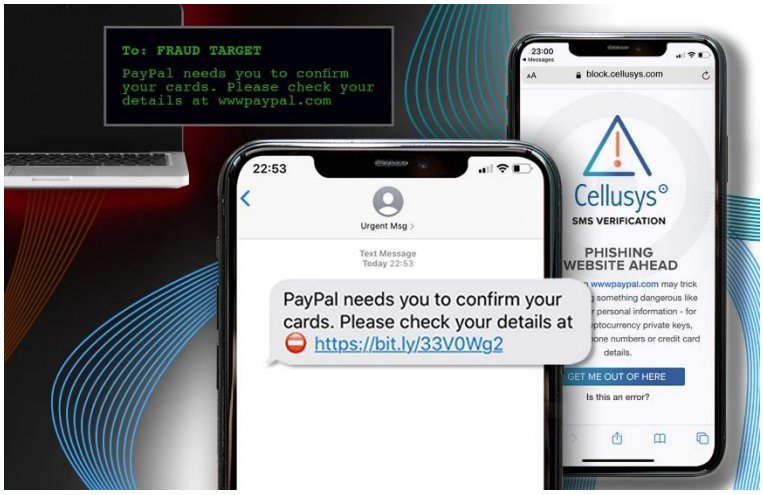
Bonnie Kimmel
PR & Marketing Manager
bonnie.kimmel@cellusys.com
+353 1 642 5000

FOR RELEASE: OCTOBER 29TH 2020

DUBLIN, IRELAND, AND VANCOUVER, CANADA

Cellusys launches SMS Verification to eradicate smishing and mobile fraud

Cellusys and MetaCert pioneer the use of Zero Trust and real time security to help mobile network operators combat SMS phishing and fraud.



Malicious URL is blocked and mobile subscriber is kept safe.

Cellusys, a leading telecom solutions provider, has partnered with internet security firm MetaCert to provide a world-first SMS security solution, using Zero Trust methodology to combat cyberattacks such as phishing, malware and financial fraud.

During the COVID-19 pandemic, SMS is being used by financial services companies and government institutions to contact people offering assistance and advice. Many mobile networks offer subscribers

ineffective or no protection against fraudulent SMS messages. Advanced SMS firewalls are able to block many large-scale smishing attempts, however none are able to detect every new threat.

Phishing is favoured by cybercriminals because it's cheaper, easier and faster to exploit a human, especially when working remotely, than it is to exploit a computer system or computer network. 'Smishing' (or SMS phishing) is a term that has been in common use since 2006.

Criminals are sending SMS messages claiming to come from government authorities demanding payment of bogus fines or offering fake financial help, while others use contact tracing as a means of tricking consumers into opening dangerous URLs. Tens of millions of dollars are defrauded from customers each year by impersonating banks across the globe, from Australia to Ireland.

According to a study by Google and the University of Florida, URLs used in targeted phishing scams like the one carried out on Twitter, only need to be active for 7 minutes for criminals to achieve their objective.

URLs used in bulk phishing campaigns only require 13 hours to do most harm, the study found. Network operator Orange Poland also recently found that 80% of customers open phishing links inside SMS messages within the first 15 minutes, while only 10% wait until the following day, which demonstrates that SMS is a perfect channel to launch a fraud attack.

"300 million domains are registered every year, with a new phishing URL created every 20 seconds. It's mathematically impossible for any company to detect and block every known dangerous URL before harm has been done.

"Mobile phone users will always be exposed to fraud and malware as long as networks continue to focus on filtering out known danger instead of telling consumers when they're safe", MetaCert CEO Paul Walsh explains.

Mobile operators claim their ability to identify and block an attack "within 24 hours," but Cellusys now provides a security system that works in real-time. With the new approach from Cellusys, every URL contained in an SMS message is checked against MetaCert's threat intelligence system and links categorized as "dangerous" are immediately blocked.

Uniquely, "unknown URLs" are similarly assumed to be dangerous. Carriers can either redirect customers to a warning page, provide a strong warning SMS, or block access to URLs that are not verified.

This approach to web access reduces the risk of a phishing-led cyberattack by more than 98% because consumers are able to make better informed choices about who to trust whenever they open an SMS message.

With an established presence in the carrier space and enterprise-grade infrastructure from Cellusys, consumers can now be protected from SMS-related fraud using the same approach thanks to their partnership with MetaCert.

"Giving subscribers this kind of visibility increases their loyalty to the network, and is a very different kind of smishing solution." said Brendan Cleary, CEO Cellusys "Adding MetaCert's technology to our

portfolio has generated a great deal of interest from networks, as an enhancement to the anti-fraud capabilities of our SMS Firewall."

"While the safety of consumers is our main priority, the increase in consumer trust should not be underestimated by carriers. Consumers who feel safe whenever they open a message with verified URLs will be more likely to trust and engage with brands. Being able to protect both consumers and brands at the same time is now a reality," Cleary added.

The solution is currently in beta and expected to go live before the end of 2020. Live customer demos are available and being demonstrated across the world.

About Cellusys

Cellusys revolutionised telecom security with the introduction of the signalling firewall in 2015. Cellusys has grown to become a Tier 1 telecom solutions provider, offering over 60 mobile networks including MTN, Vodafone, and Tata solutions for signalling security, A2P monetisation, roaming, analytics, and IoT. Cellusys systems improve quality of service and security for over 800 million subscribers worldwide, and make mobile networks more secure, intelligent and profitable.

About MetaCert

MetaCert is an open security protocol for the internet, storing trust and reputation information about Uniform Resource Identifiers (URIs) including domain names, applications, bots, digital wallet addresses, Application Programming Interfaces (APIs), and content classification. MetaCert is the first company to enable a Zero Trust strategy for web access with browser-based security software that protects organisations from the world's most sophisticated phishing-led cyberattacks.

###

Notes to Editors

NHS SMS fraud awareness alert:

https://cfa.nhs.uk/resources/downloads/fraud-awareness/covid-19/COVID-19_SMS_and_Text_Message_Scams.pdf

US SMS contact tracing SMS scam alert:

https://www.consumer.ftc.gov/blog/2020/05/covid-19-contact-tracing-text-message-scams

Report of Australian SMS phishing scam:

https://www.itnews.com.au/news/two-arrested-over-large-scale-sms-phishing-scam-553829

Alert about Bank of Ireland customers targeted by phishing scam:

https://www.osintme.com/index.php/2020/07/18/new-phishing-campaign-aimed-at-bank-of-ireland-users/

Google and University of Florida study of phishing:

https://elie.net/talk/deconstructing-the-phishing-campaigns-that-target-gmail-users/

UK efforts to identify and block phishing attacks within 24 hours:
https://newscentre.vodafone.co.uk/news/beware-covid-19-smishing-text-message-scams/

Orange Poland findings:

https://www.cert.orange.pl/aktualnosci/raport-cert-opl-sms-czyli-krotka-wiadomosc-phishingowa

Source for the number of new domains created every year:

https://www.websitehostingrating.com/internet-statistics-facts/

Source for the frequency of new phishing URLs being created:

https://www.wandera.com/mobile-threat-landscape/

Cellusys and MetaCert press pack

https://www.dropbox.com/sh/nb5byg4r6p68t6k/AAC12kmxMzjcNEtW-GtCS8Tva?dl=0