

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- ▼ [Security Architecture](#)
  - [Cloud Security](#)
  - [Identity & Access](#)
  - [Data Protection](#)
  - [Network Security](#)
  - [Application Security](#)
- ▼ [Security Strategy](#)
  - [Risk Management](#)
  - [Security Architecture](#)
  - [Disaster Recovery](#)
  - [Training & Certification](#)
  - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [Cybercrime](#)



## Phishers Add Chatbot to the Phishing Lure

By [Kevin Townsend](#) on May 19, 2022

Share

Tweet

推荐 0



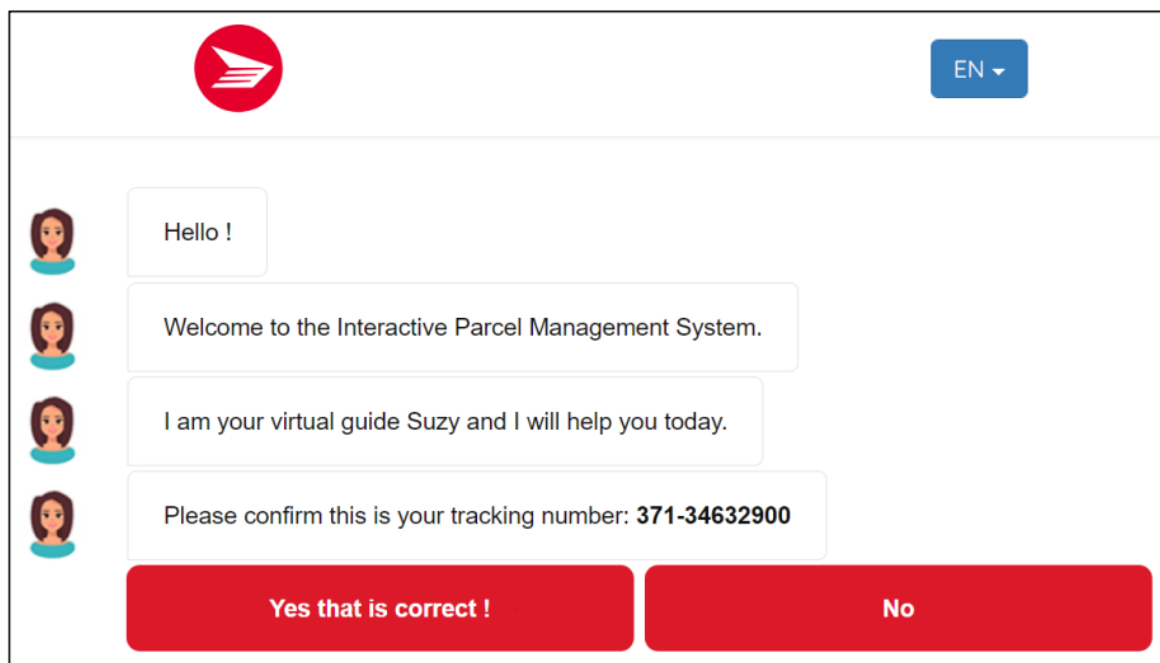
Researchers have discovered a new approach being taken by phishers to increase victim engagement and confidence: the addition of an interactive chatbot. We have all become accustomed to the chatbots used by many of the largest service providers - they are annoying, but something we must navigate.

The phishers hope that this reluctant acceptance of chatbots will help lower the attention of the target victim. The process is described in a new [blog](#) post.

The discovery was made at Trustwave SpiderLabs. In its own telemetry it has found just the one sample, but Karl Sigler, manager of SpiderLabs' threat intelligence notes that since the phishers have registered a series of domains for the process, it is likely to be part of a wider campaign.

The basic lure is the common failed DHL delivery, and the victim must still fall for this. But the victim is not immediately directed to the phishing site. Instead, the 'please follow our instructions' results in the delivery of a PDF with a 'fix delivery' button. So far, although there are red flags for the observant victim, there is nothing overtly dangerous.

If the victim clicks the button, he or she is sent to another website where the phishing chain begins with the introduction of a chatbot that promises to fix the delivery but really harvests personal data.



If the target accepts the chatbot, it continues the engagement by showing the victim a photo of the damaged package, and asks for details on how to deliver. If the victim asks to schedule delivery, a false CAPTCHA is presented to further increase confidence.

The next stage is to ask for a delivery address and time. An unspecified password is requested. It really doesn't matter what password is entered - it could be a DHL account password or the user's email account - the phisher steals it anyway along with the delivery address and the user's email address (which he already has). The phishing has begun but is not complete.

The chatbot explains that the additional delivery attempt is an additional service that requires payment - so a credit card payment page is displayed. The amount is small. If the victim has been taken in so far, the payment is not unreasonable. Paying for the fake redelivery gives up the phisher's real target - bank card details.

There then follows a strange procedure - the phisher says an OTP verification code has been sent to the victim. But the phisher hasn't yet asked for the victim's phone number, so this could not happen. "Putting in random characters will just redirect you to the same page stating that the security code is no longer valid," write the researchers. "On the fifth try, however, the page redirects to another page saying that the submission was successfully received. This marks the end of the perpetrator's phishing chain."

We are left with a somewhat puzzling phishing attack. It seems sophisticated but lacking in some very easy detail that could improve it. It would be easy, indeed logical, to ask for the victim's phone number for the OTP token. The fact that the chatbot is going to send a token to a phone number that hasn't been given could be a serious red flag. At the same time, the phisher no longer really cares since he already has the details he was after.

However, an apparently functioning OTP would give the victim greater confidence in the validity of the process. With no concerns, the victim may easily give no further thought to the occurrence until non-delivery of the non-existent package (if ever) - giving the phisher ample time to collect the user details. The obviously flaky OTP process, could, however, spark sufficient concern for the victim to contact his or her bank.

This combination of sophistication with a certain level of incompleteness raises the question of whether this is really an attack methodology still in development. It is certainly possible that this sample will mark the beginning of a wider and more sophisticated use of chatbots in phishing campaigns. However, Trustwave's Sigler has a slightly different view.

“Reading through the lines and with my experience,” he told *SecurityWeek*, “what this tells me is that this was a campaign first used for other purposes. They probably did have it more targeted; they probably did ask for the potential victim’s phone number and then sent them an OTP code to try and capture that. But what the phishers are doing here is they’re reusing the same infrastructure from a more targeted campaign for more general purposes. This could be some minor group that just bought this package from some malware-as-a-service or some dark web link and are trying their best to use it as they can, even though certain components of it don’t really make sense to the victims they’re targeting.”

**Related:** [SaaS App Vanity URLs Can Be Spoofed for Phishing, Social Engineering](#)

**Related:** [APT Group Using Voice Changing Software in Spear-Phishing Campaign](#)

**Related:** [FBI Warns of Phishing Attacks Targeting US Election Officials](#)

**Related:** [Cybercriminals Using GitHub to Host Phishing Kits](#)

Share

Tweet

推荐 0



Kevin Townsend is a Senior Contributor at SecurityWeek. He has been writing about high tech issues since before the birth of Microsoft. For the last 15 years he has specialized in information security; and has had many thousands of articles published in dozens of different magazines – from The Times and the Financial Times to current and long-gone computer magazines.

Previous Columns by Kevin Townsend:

[Phishers Add Chatbot to the Phishing Lure](#)

[QuSecure Lauches Quantum-Resilient Encryption Platform](#)

[The Vulnerable Maritime Supply Chain - a Threat to the Global Economy](#)

[Zero Trust Firm Xage Security Adds \\$6 Million 'Top-up' to \\$30 Million Series B Funding](#)

[Ransomware Attack a Nail in the Coffin as Lincoln College Closes After 157 Years](#)

[2022 CISO Forum: September 13-14 - A Virtual Event](#)

sponsored links

[2022 ICS Cyber Security Conference | USA \[Hybrid: Oct. 24-27\]](#)

[Virtual Event Series - Security Summit Online Events by SecurityWeek](#)

[2022 Singapore/APAC ICS Cyber Security Conference](#)

Tags:

[NEWS & INDUSTRY](#)

[Cybercrime](#)

Search

**Get the Daily Briefing**

**BRIEFING**

Business Email Address

Subscribe

