CORRECTION

Correction to: Social Engineering Attacks During the COVID-19 Pandemic

Venkatesha Sushruth¹ · K. Rahul Reddy¹ · B. R. Chandavarkar¹

Published online: 11 March 2021
© Springer Nature Singapore Pte Ltd 2021

Correction to: SN Computer Science (2021) 2:78
<https://doi.org/10.1007/s42979-020-00443-1>

In the original publication of the article, the production team processed figure captions incorrectly for the Fig. 2 to 10. The correct figure captions are given below:

Fig. 2 Accounts that received a “government-backed attacker” warning each month of 2020 [9]

Fig. 3 Spending by business on software during the early stages of the COVID 19 pandemic [14]

Fig. 4 Number of customers on online platforms increased for most product due to COVID-19 [17]

Fig. 5 Outline of a credential phishing attack [20]

Fig. 6 Outline of a business email compromise attack [20]

Fig. 7 COVID-19 themed SEAs [10]

Fig. 8 Modifications to phishing emails in response to the pandemic [24]

Fig. 9 Phishing email impersonating the WHO [19]

Fig. 10 Phishing SMS [23]

The original article has been corrected.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

The original article can be found online at <https://doi.org/10.1007/s42979-020-00443-1>.

✉ Venkatesha Sushruth
vsushruth21@gmail.com

K. Rahul Reddy
k_rahul_reddy@outlook.com

B. R. Chandavarkar
brcnitk@gmail.com

¹ Department of Computer Science and Engineering, National Institute of Technology Karnataka, Surathkal, Mangalore, India