

Aware Force says beware of online scammers urgently asking for cash to help the people of Ukraine

Make sure you research the organization asking for your money by using the tips below in this news release.

The logo for Aware Force, featuring the word "Aware" in black, a red stylized "A" with a swoosh, and the word "Force" in black with a registered trademark symbol.

Employee cyber security engagement firm Aware Force

ATLANTA, GEORGIA, UNITED STATES,
March 17, 2022 /EINPresswire.com/ --

Online scammers are playing on the sympathies of those who want to help Ukrainian citizens with bogus appeals for cash that instead goes directly into scammers' pockets, according to Atlanta-based employee [cybersecurity awareness](#) and engagement firm [Aware Force](#).

“

Regardless of your age or education, you will be receiving more texts, e-mails, and even phone calls asking urgently requesting help for Ukrainian citizens. Make sure the right people get your money.”

Richard Warner

“Ukraine is a global crisis that is motivating millions to help. Scammers know that. They’re using automation to customize their emails and texts to victims. The messages are designed to look genuine, but they’re not,” says [Richard Warner](#), Founder, and CEO of Aware Force.

Research by Aware Force shows that scammers customize their fake messages by trolling a victim’s Facebook feed and other social media accounts to learn information about the target and the names of friends. Scammers use this personalized information to send convincing messages on platforms like WhatsApp.

Warner gives this advice to avoid bogus Ukrainian aid phishing emails and texts:

- Use the “Blood Pressure” rule: if you receive an email or text message that raises your blood pressure because it shows graphic images of death, destruction, and tragedy, slow down and be suspicious.
- Is the message urgent? Does it relate to something personal, such as an alma mater or placement of employment? Those are other reasons to be skeptical.
- Don’t click on links in emails or texts about Ukraine-related donations. Instead, use a search

engine to find out about the organization. If the organization doesn't appear in search results, ignore it.

- If the link in an email or text is a jumble of letters and numbers, it's likely a scam.
- Just delete these messages. Don't unsubscribe. Clicking on an "unsubscribe" link or replying to a text with "STOP" only alerts scammers that someone is reading the message.
- Check the "privacy" settings on your social media accounts. Make sure only friends can see what you post, not "friends of friends" or the general public.
- Visit www.scamadvisor.com from the Global Anti-Scam Alliance, which tracks worthy nonprofits that are, in fact, helping Ukraine.

The Netherlands-based GASA says people with advanced degrees and higher levels of education are being taken for more money than high school grads. And they say millennials are more apt to be scammed than seniors.

"Regardless of your age or education, you will be receiving more texts, e-mails, and even phone calls asking urgently requesting help for Ukrainian citizens," declares Warner. "Make sure the right people get your money."

Richard Warner

Aware Force

+1 404-822-3309

[email us here](#)

Visit us on social media:

[Twitter](#)

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/565741411>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2022 IPD Group, Inc. All Right Reserved.