HC3: Sector Alert

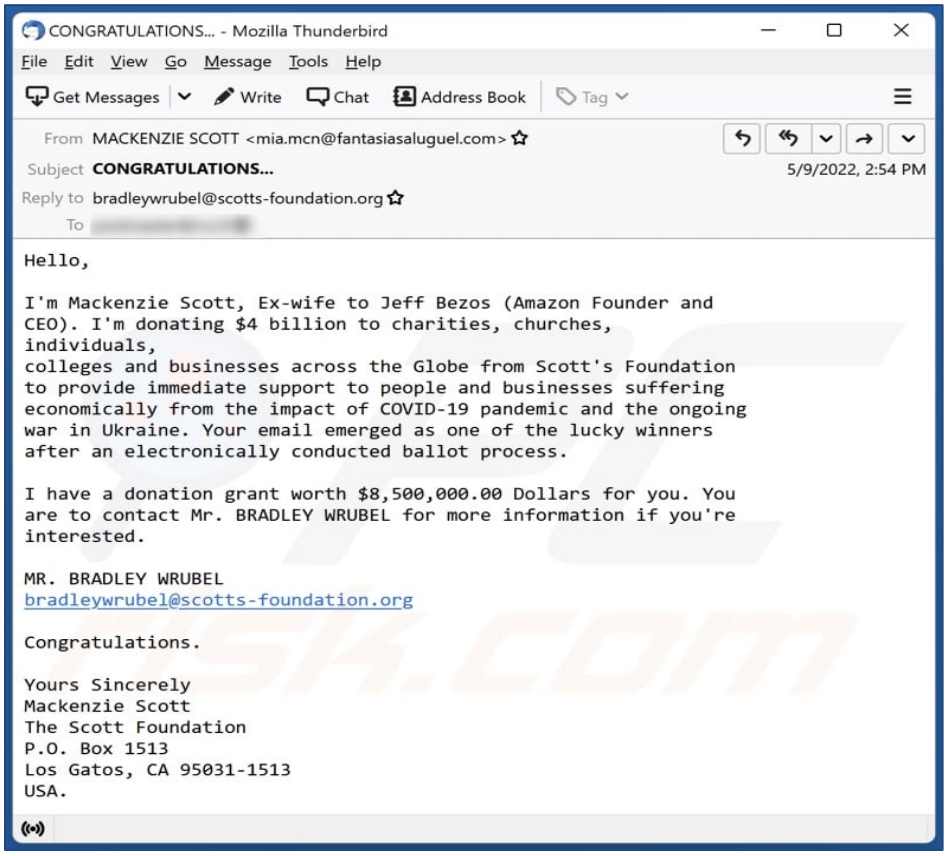
August 16, 2024 TLP:CLEAR Report: 202408161700

Grant Donation Email Scam

Executive Summary

A grant donation email scam attempts to trick individuals and businesses experiencing economic setbacks into believing that they will receive a large sum of money. These scams claim that the recipients' emails were selected as winners in a randomized process. The damage from falling victim to one of these scams can be loss of personally identifiable information (PII) or private heatlth information (PHI), monetary loss, identity theft, and more. HC3 is aware of several instances of this scam currently affecting the U.S. HPH sector and strongly advises exercising caution with incoming emails and messages.

Report



Example of a grant donation scam email. The scammer is purporting to be philanthropist Mackenzie Scott. *(Source: PCRisk)*

Typically, grant donation scams work in two ways—as phishing, or as a deception intended to lure money out of the victims—and they promise funds, rewards, or prizes, often requesting victims to make payments for bogus reasons like fake shipping, storage, transactions, or other fees. Phishing scams target a wide variety of information like personally identifiable details (PII), addresses, telephone numbers, email addresses, banking account numbers, credit card details, log-in credentials, and more. This vulnerable information can be used to craft personalized scams or can be sold to third parties. Additionally, these emails can contain infectious files as attachments or download links. These files can be in various formats: executables, archives, PDF, Microsoft Office documents, JavaScript, etc. When a virulent file is

HC3: Sector Alert

August 16, 2024 TLP:CLEAR Report: 202408161700

Patches, Mitigations, and Workarounds

To avoid falling victim to grant donation scams, HC3 has these recommendations:

- **Use strong passwords and enable two-factor or multi-factor authentication.** Encourage the use of complex and unique passwords for all accounts, and discourage the sharing of passwords. Implement two-factor or multi-factor authentication on all accounts whenever possible. This provides an extra layer of security by requiring a second verification step.
- **Exercise caution when opening emails or clicking on links.** Especially if they are from unknown senders. Avoid downloading attachments unless they are expected and from trusted sources.
- **Do not give your information to an unsecured site.** If the URL of the website does not start with "https" or a closed padlock icon next to the URL is not visible, do not enter any sensitive information or download files from that site. Sites without security certificates may not be intended for phishing scams, but it is better to be safe than sorry.
- **Implement anti-phishing tools.** Use anti-phishing tools and technologies that can detect and block fraudulent websites and emails. Firewalls are an effective way to prevent external attacks, acting as a shield between a computer and an attacker. Both desktop firewalls and network firewalls, when used together, can bolster security and reduce the chances of a hacker infiltrating an organization's environment.
- **Conduct security awareness training.** It is impossible to solely rely on technical measures to prevent phishing attacks, which is why security awareness training is crucial. This training should educate employees on the harm of phishing and empower them to identify and report suspicious attempts. Simulated phishing campaigns can further reinforce the training, allowing organizations to assess their own risk and improve workforce resiliency. It is important to communicate with employees when they click on simulated phishing emails, emphasizing the risks and reminding them how to report suspicious emails.

References

How to Prevent Phishing Attacks: 10 Ways to Avoid Them
https://www.lepide.com/blog/10-ways-to-prevent-phishing-attacks/

"Lee Shau Kee Foundation" Donation Scam
https://www.onlinethreatalerts.com/article/2018/3/29/beware-of-the-lee-shau-kee-foundation-donation-scam/

What kind of email is "Donation Grant For You"?
https://www.pcrisk.com/removal-guides/23817-donation-grant-for-you-email-scam

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback