What you need to know about

Russia-Ukraine Conflict Phishing Scams

As the conflict in Ukraine unfolds, threat actors are using this current event as a lure in phishing emails.

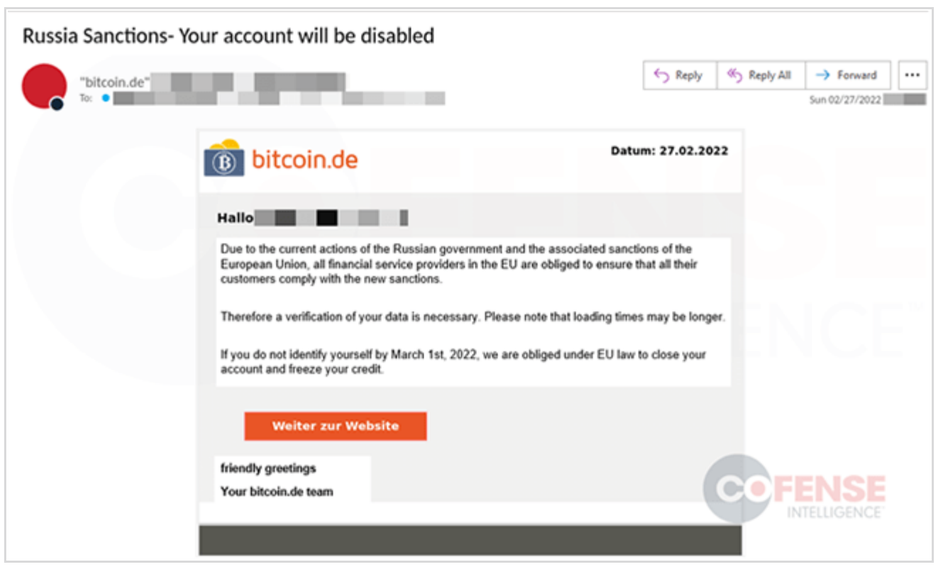
No Topic is Off Limits

Threat actors use newsworthy topics to entice targets to click links, open attachments, or divulge credentials. To compel targets to take action, threat attackers appeal to strong emotions like shock, anger, curiosity, fear, and sense of urgency.

Example 1: Sanctions-Themed-Email Targeting Cryptocurrency Marketplace Credentials

This phishing email used the subject of sanctions against Russia to target employees at a European financial service provider.

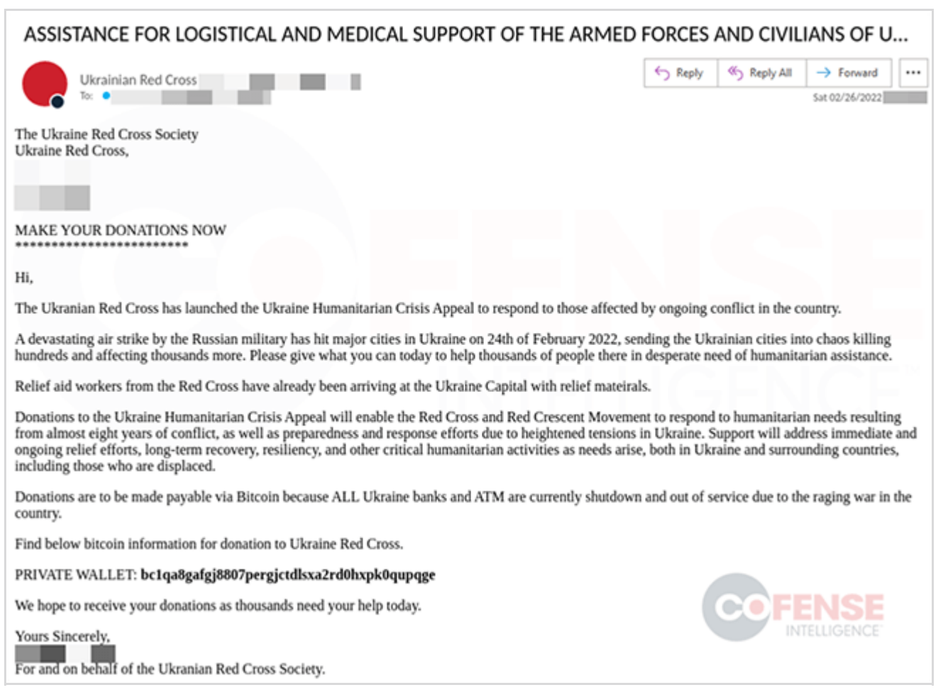
The campaign spoofs the login page of popular German Bitcoin marketplace bitcoin.de, targeting login credentials with the likely intention of stealing cryptocurrency.



English translation of a bitcoin.de-spoofing email with Russian Sanction lure.

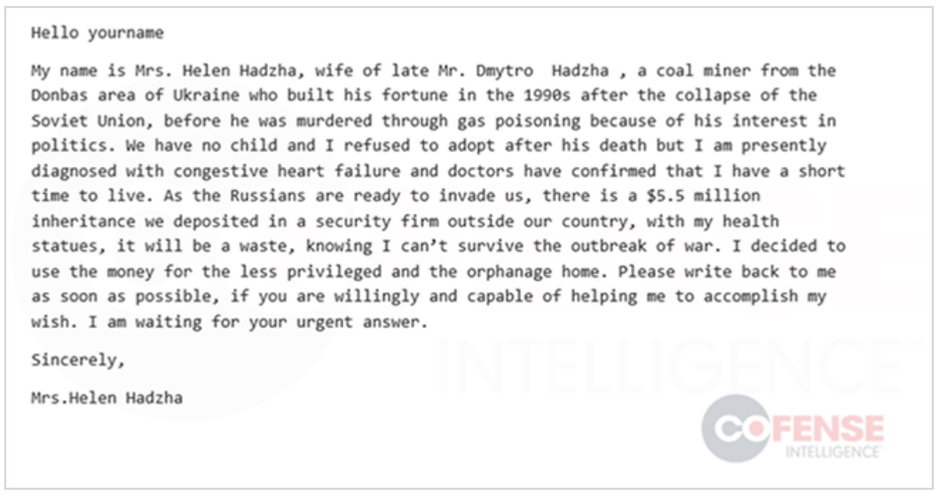
Example 2: Humanitarian-Aid-Themed Scam Seeks Cryptocurrency

This phish spoofs the Ukraine Red Cross Society, aiming to scam donors into cryptocurrency donations to a private wallet. The scam claims that funds will be used for logistical and medical support of Ukraine armed forces and civilians.



Example 3: Humanitarian-Aid-Themed Scam Seeks Cryptocurrency

This phish spoofs the Ukraine Red Cross Society, aiming to scam donors into cryptocurrency donations to a private wallet. The scam claims that funds will be used for logistical and medical support of Ukraine armed forces and civilians.



Remember:

1. **Think Twice.**
   Attackers will use emotional appeals in their emails. Stay calm and look closely at the email content before responding.

2. **Examine Links and Domains**
   Look closely at URLs and domains in emails to make sure they are correct. Also, look for misspellings.

3. **Guard Your Credentials**
   Keep your usernames, passwords, and security questions and answers private. If you suspect that you've logged into a website that didn't authenticate your credentials, first reset your password, and then report it to your Help Desk.

4. **Always Verify**
   Make sure the sender's email address matches who it is coming from.

Report Phishing

Remember, you are the last line of defense against phishing.
If you receive a suspicious email, report it immediately.