ARMY CRIMINAL INVESTIGATION DIVISION

20 November 2024

# Cybercrime Prevention Flyer

## Pegasus Email Scam - Financial Extortion Through Intimidation

**Background**

Cybercriminals are up to their usual tactics, sending phishing emails to unsuspecting victims. However, there is a twist to a recent wave of phishing emails.

After sending a seemingly personalized email with false claims to have installed a spyware called Pegasus on the victim's cellphone, the cybercriminal accuses the victim of visiting pornographic sites and claims to possess embarrassing footage of the victim. To enhance the believability of the scam, the cybercriminal includes the victim's name and an image of their home in the phishing email.

Creating a sense of urgency, the cybercriminal gives the victim a short deadline to pay a ransom, via a QR code linked to a cryptocurrency address, or suffer the embarrassment of released compromising footage and browsing history to family and friends.

**Why the Scam Works**

Part of the success of the Pegasus email scam is that the Pegasus Spyware does exist. Pegasus can compromise both iOS and Android devices, turn on and off cameras and microphones, record phone calls, reveal text messages, photos, emails, contact lists, and videos stored on the devices, and more. The fear of someone having control of one's cellphone can impact rational thinking.

The other factor making this phishing scam successful is that it includes the victim's name and an image of their home in the email. However, this does not mean the recipient is a victim of identity theft. Individual's names and contact information, to include email addresses, are often publicly available, including property images that can be captured using Google Street View.

**What the Email Looks Like**

Here is an example of a Pegasus phishing email. Note how the cybercriminal speaks directly to the target and creates a sense of urgency.

It's important you pay attention to this message right now. Take a minute to relax, breathe, and really dig into it. We're talking about something serious here, and I don't play games. You don't know anything about me whereas I know ALOT about you and you must be wondering how, right?

Well, You've been treading on thin ice with your browsing habits, clicking through those adult videos and venturing into the darker corners of cyberspace. I actually placed a Spyware called "Pegasus" on a app you frequently use. Pegasus is a spyware that is designed to be covertly and remotely installed on mobile phones running iOS and Android. And while you were busy watching our videos, your device began functioning as a RDP (Remote Control) which provided me complete accessibility to your device. I can look at everything on your display, flick on your cam and mic, and you wouldn't have a clue. Oh, and I have got access to all your emails, contacts, and social media accounts too.

**What I want?**

Been keeping tabs on your pathetic life for a while now. It is just your hard luck that I got to know about your blunder. I gave in more time than I probably should have digging into your life. Extracted quite a bit of juicy info from your system. and I've seen it all. Yeah, Yeah, I've got footage of you doing embarrassing things in your house (nice setup, by the way). I then developed videos and screenshots where on one side of the screen, there's the videos you were enjoying, and on the other part, it is your vacant face. With simply a click, I can send this filth to all of your contacts.

### Recognize Phishing Emails

- **Threatening Email with Urgent Action Required.** Be suspicious of threatening emails that require immediate action or consequences will be dire.
- **Poor grammar and Spelling.** If the email is poorly written or has obvious spelling or grammatical errors, it might be a scam. Be aware, cybercriminals are using artificial intelligence (AI) to correct errors and make emails appear legitimate. Even a well written email could be a scam.
- **Suspicious Sending Email Address.** If the sender's email address is not recognized or appears to be from a known company but looks odd, attempt to verify the email address.
- **Unsolicited Links and Attachments.** If an email contains unrequested links or attachments, be suspicious and do not click on the link or open the attachment.
- **Personal or Financial Information Requests.** Be cautious of emails requesting confirmation of personal or financial information when you did not initiate the request.

### What to Do with Phishing Emails

- If the sender or company is unknown, the email is unexpected, and links or attachments in the email are suspicious, flag the email as spam or delete the email.
- If the email appears suspicious but the sender or company is known, contact the sender using a known or verified phone number or email address to determine the authenticity.
- Avoid clicking on links or downloading attachments.
- Do not reply to the sending email address.
- Report it.

If you are a victim of the Pegasus email scam and affiliated with the U.S. Army, notify the Department of the Army Criminal Investigation Division (DACID) via the Submit a Tip – Report a Crime website or directly to the DACID Cyber Field Office by email. If you are not affiliated with the U.S. Army but a victim of the Pegasus email scam, report the incident to the Internet Crime Complaint Center.



To receive Cyber Field Office Cybercrime Prevention Flyers, send an email to: CYDIntel@army.mil

CPF 0103-2024-CID461

Cyber Field Office
Russell Knox Building
27130 Telegraph Road
Quantico, VA 22134