

CPF 0008-2020-CID361-9H

24 April 2020

Internet Email Scams

Still bouncing around the internet is a [blackmail scam](#) the Major Cybercrime Unit (MCU) shared with you a year ago.

An email arrives in your inbox that lists your password or at least a password you've used before. The sender explains they have live recorded videos of you watching and enjoying online pornography, cheating on your spouse, or some other taboo behavior.

It was purportedly recorded by your computer's webcam. A virus or malware placed on your computer detected one of a range of explicit activities and activated your webcam.

The sender threatens to send the video to your family and friends if hush money is not paid immediately. Currently, the amount being reported to MCU is \$2,000. The sender demands you must pay that money in virtual currency, usually Bitcoin.



You can spot these scam emails; many of their traits are common among various email fraud schemes.

Common Traits

- The email comes from someone you don't know.
- The English and grammar are poor. Words and punctuation are often incorrect.
- The email claims your computer was infected with malware, adware, or viruses that were used to capture the video.
- The email threatens to send the video to friends and family.
- Payment must be made in Bitcoin, which, by the way, is untraceable.

Recommendations

- Do put a piece of opaque tape over your webcam when not using it.
- Do delete scam emails — do not click on any links in the emails. Report all scam emails to the [Internet Crime Complaint Center](#).
- Do not pay money. If you paid money or transferred Bitcoin, contact your local FBI office, CID, or local police.
- Do install, use, and update antivirus software. DoD employees can download no-cost antivirus software for home use from the [Department of Defense Patch Repository](#) site.
- Do change your passwords.
- Do use [strong passwords or passphrases](#).
- Do not reuse passwords.
- Do not use "password" or "123456" or any other easily guessed password. (Do people really do that? [YES](#).)



**Report a crime to U.S. Army
Criminal Investigation Command**

Major Cybercrime Unit

**27130 Telegraph Road
Quantico, Virginia 22134**

Email

MCU Web Page

CID LOOK OUT
ON POINT FOR THE ARMY

DISTRIBUTION:

**This document is authorized for the
widest release without restriction.**



"DO WHAT HAS TO BE DONE"

If you've ever wondered how someone can make money off this kind of scam, consider the following:

- A reliable online site claims to have more than 9.5 billion username/password combinations.
So, if
 - the scammer's threatening email reaches just one one-hundredth of one percent of those email addresses,and,
 - if just one one-hundredth of one percent of that initial one one-hundredth of one percent sends \$2,000,then, the cybercriminal earns about **\$200,000!**

A recently received scam email.

It seems that, _____, is your pass word.

I need your total attention for the next Twenty-four hrs, or I will certainly make sure you that you live out of shame for the rest of your life.

Hello there, you do not know me. But I know just about everything regarding you. Your current fb contact list, phone contacts plus all the virtual activity in your computer from past 175 days.

Including, your masturbation video footage, which brings me to the primary motive why I am composing this specific email to you.

Well the last time you went to see the porno online sites, my spyware ended up being triggered in your computer which ended up recording a beautiful footage of your self pleasure act simply by triggering your cam.
(you got a incredibly strange taste by the way haha)

I have got the entire recording. If perhaps you feel I am playing around, just reply proof and I will be forwarding the recording randomly to 7 people you know.

It may end up being your friend, co workers, boss, parents (I don't know! My system will randomly choose the contacts).

Would you be capable to look into anyone's eyes again after it? I question that...

But, it does not need to be that path.

I want to make you a one time, no negotiable offer.

Buy USD 2000 in bitcoin and send it to the below address:

[case-SENSITIVE copy & paste it, and remove * from it]

(If you don't understand how, lookup how to purchase bitcoin. Do not waste my valuable time)

If you send this 'donation' (let's call it that?). Immediately after that, I will disappear and under no circumstances make contact with you again. I will erase everything I have got about you. You may carry on living your current regular day to day life with no stress.

You have 1 day in order to do so. Your time will start as soon you go through this mail. I have an unique program code that will alert me as soon as you go through this e mail so don't attempt to play smart.

Email Scams in the News

[How Not to Fall Prey to Email Threats](#) – USA Today

[How to Avoid Bitcoin Scams](#) – Federal Trade Commission

[Ask Jack – I received a phishing email. Now what?](#) – The Guardian

Reporting Cybercrimes

[U.S. Department of Justice](#)

[Internet Crime Complaint Center](#)

To receive future MCU Cybercrime Prevention Flyers, send an email to: [Subscribe CPF](#)

Disclaimer: The appearance of hyperlinks in this Cybercrime Prevention Flyer, along with the views and opinions of authors, products or services contained therein do not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations.