U.S. ARMY
CYBER COMMAND

www.arcyber.army.mil | Follow @arcyber

Extortion Emails

WHY DO HACKERS OFTEN USE EMAIL TO LAUNCH ATTACKS OR SCAMS?

Mail servers and computer workstations running mail clients are frequently targeted by malicious attackers and cyber criminals. Because the computing and networking technologies that underlie email are ubiquitous, attackers are sometimes able to develop attack methods to exploit security weaknesses in even the best systems.

Mail servers are also targeted because they (and public Web servers) must communicate to some degree with untrusted third parties. Email clients are also targeted as an effective means of inserting malware into a machine and spreading it to other machines.

HOW DO EXTORTION EMAILS WORK?

Government systems with Defense Enterprise Email are protected by a variety of security gateway and filtering technologies. However, malicious attackers still occasionally find ways to slip past these guardians. And whether the attack is on government or personal systems, their goal is often to commit extortion and blackmail users for profit.

Blackmail emails may use a variety of threats to attempt to coerce users. Often they include the recipient's personal username and password, culled from the Internet or the dark web after being stolen in data breaches. The sender demands money and threatens to expose the recipient's information or browsing habits if not paid. Or the blackmailers may claim to have taken over the user's webcam and recorded compromising video that will be released if they are not paid. Often payment is demanded in cryptocurrency such as Bitcoin, money transfers or gift cards that may be difficult or impossible to trace.

WHAT CAN I DO TO PROTECT MYSELF AGAINST EMAIL EXTORTION?

There are some things users can do -- or should avoid doing -- to lessen their chances of becoming a victim.

Some things you CAN do:

- If you get a threatening email, do a web search for a phrase or two from the email to see if it's a spam message that has been sent to a large number of people or has been reported to U.S. government databases
- Change the password you use for a website you've learned has been hit by a data breach
- Use two-factor or multi-factor authentication when they are available. These require you to provide something in addition to a password to enter a website, such as a security code or authenticator application on your device, and prevent access accounts with just a stolen password
- Keep your operating system, web browser and antivirus programs up to date
- Cover the lens on your webcam when you're not using it, to thwart hackers might try to use it to spy on you

Some things you should AVOID doing:

- Don't reply to extortionist's emails
- Don't pay blackmailers in the hope that they will go away; they may just respond by demanding more money
- Don't keep using a password that scammers mention in their threatening emails -- change it immediately
- Don't use the same password for multiple sites; if you have trouble keeping track of multiple passwords, use a password manager program
- Don't click any links or open attachments in an extortion emails; they could be ploys to infect your computer with malware.
- Don't immediately delete scam emails -- hold onto them for reporting purposes

That last point is vital -- if you are victimized by a blackmailer, report the incident as soon as possible.

Attacks on government email or systems should be reported to the user's Information Assurance and security officials.

Malicious attacks on personal systems can be reported to the Federal Bureau of Investigation's Internet Crime Complaint Center at https://www.ic3.gov/default.aspx or the Federal Trade Commission at https://www.ftc.gov/faq/consumer-protection/submit-consumer-complaint-ftc