Cybercrime Prevention Flyer

Contact Information:
Cyber Criminal Intelligence Program
27130 Telegraph Road
Quantico, Virginia 22134

Phone: 571.305.4482 [DSN 240]
Fax: 571.305.4189 [DSN 240]

Email

CCIU Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

"Do What Has To Be Done"

CPF 00005-19-CID361-9H **27 March 2019**

Blackmail Emails

It arrives in your inbox. The email sender lists one of your usernames and passwords. There's a demand for money.

You read on and learn malware was installed on your computer when you visited a *certain kind* of internet site. The malware captured your username and password. Your visits to those websites will be exposed if you do not pay hush money.

And, the username and password are ones you have used before. Your first thought? "It must be real. How else would they know my username and password?"

This is a scam. Do not engage the sender. Do not pay the ransom.

Much of your personal information, including your first and last names, email addresses, and usernames and passwords, is spread across the internet. If you are an internet user, it is almost inevitable.

Often, the information has been stolen in a data breach and then posted on internet sites intended to expose your personal information. Cybercriminals know where to find this information and how to weaponize it.

Most likely, the usernames and passwords you see in the email you received have been lifted from one of the thousands of breaches and millions of exposed customer records.

In 2018 alone, there were 1,244 breaches (that's down 23% from 2017) and more than 400 million customer records exposed (that's up 126% from 2017).

The variety of industries and types of businesses impacted by [data] breaches in 2018 opened the eyes of many consumers to the fact that breaches have become "the new normal". It's not so much a matter of "if" a breach will happen, but "when" a breach will happen.

2018 End of Year Data Breach Report
Identity Theft Resource Center

The scammer threatens to expose browsing habits unless hush money is paid. Oftentimes the scammer demands payment in the form of bitcoin, money transfers (think Western Union and MoneyGram) or gift cards. These are at best difficult for law enforcement to trace. At worst, they are impossible to trace.

Cybercrime Prevention Flyer

Recommendations

- 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 anti-virus software. DoD employees can download no-cost antivirus software for home use from Defense Information System Agency, AV/AS site.
- Do change your passwords.
- Do use strong passwords or passphrases.
- Do not reuse passwords.
- Do no use “password” or “123456” or any easily guessed password. (Do people really do that? YES.)
- Do not reuse passwords.

In the News

2018 End of Year Data Breach Report – Identity Theft Resource Center

Scammers Pretend They’ve Watched You – Newsweek

FBI Warns About Cyber Blackmail Threats – Miami Herald

Don’t Fall Victim to Latest Extortion Mail – USA Today

Resources

Manipulation Tactics Used in Phishing – Help Net Security

Top 10 Tips to Secure Your Computer – University of California, Berkeley

Protect Yourself Against Phishing Scams – University of California, Berkeley

Consider Metadata When Sending Files – University of Michigan

Tips for Safe Emailing – CID

Cybercriminals Target Soldiers – CID

Extortion Scams – CID

Webcam Fraud – CID

To receive future CCIU Cybercrime Prevention Flyers, send an email to: usarmy.cciuintel@mail.mil with “SUBSCRIBE: CPF” in the subject line.

CCIU uses the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide feedback.