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 0005-18-CID361-9H **04 October 2018**

Your Webcam Could be Watching You—And You Might Not Even Know

Cybercriminals are more sophisticated than ever before. That's not difficult to understand. It's not even surprising. They learn quickly. But, oddly, that increased sophistication manifests in simpler attacks. Rather than engaging victims in lengthy grooming, cybercriminals exploit their victim's conscience and their fear of public embarrassment. The attack is quick and abusive.

You might receive an email addressed to you specifically. Sometimes the email includes one or more of your real usernames. The email seems to target you specifically! But it's not all that difficult to figure out your username. It's probably part of your email address. But it's still a little alarming. Often this blackmail looks even more convincing when it includes one of your passwords. A password you've actually used. That piece of your online identity that you've jealously protected. Never revealed to anyone. And, it's one you now use or at least have used.

> "Cybersecurity is an issue of profound importance in today's technology-driven world. What was once a problem only for IT professionals is now a fact of life for all of us… There's hardly a day that goes by that we don't hear of some new cyberattack."
>
> **Luis A. Aguliar**
> **Commissioner**
> **U.S. Securities and Exchange Commission**
> **Jun 25, 2015**

The cybercriminal claims to have accessed your computer, hijacked your webcam, and captured compromising videos of you and your family. The cybercriminal threatens to send the compromising video to your spouse, maybe relatives, and sometimes your employer. Graciously, in exchange for a payment, the criminal offers to destroy the video and tell no one.

This scam relies on shock value and exploits our innate human forgetfulness. It capitalizes on people's fear of public embarrassment and the even more frightening prospect of ruined professional standing in the community and with employers.

But realize this scam for what it is. A scam. Although it's possible for a hacker to remotely take control of your webcam and record video, it's unlikely anyone really did, because you've been following safe computing practices. You use strong passwords, you update your software and hardware with the latest version, you change your passwords from time to time, etc. But if you want to reliably ensure that your camera can't be used to record anything, CID has an elegant solution. Cover your webcam lens!

Yes. Covering your webcam lens with something opaque, something you can't see through, prevents the camera capturing anything. Take the covering off only when you intend to use the camera and then for only as long as you actually use the webcam.

If you choose to cover the lens, CID urges you to use something with low or no residue adhesive like gaffer tape or sticky notes.

Oh, and that real username, real password in the email? That probably came from one of the tens of thousands of security breaches. Oftentimes, the stolen information, which sometimes includes username, password, account numbers, and other personal information, is posted to the web for other hackers to use. It doesn't necessarily mean the criminal compromised your system.

If you receive emails like this and believe you are at risk or the threat is genuine, contact your local law enforcement agency or report the incident to the Internet Crime Complaint Center.

In the News

Don't Fall Victim to Latest Extortion Mail — USA Today

Scammers Pretend They've Watched You — Newsweek

FBI Warns About Cyber Blackmail Threats — Miami Herald

Police Warn of Blackmailing Scam — Iceland Review

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

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