

CPF 00008-2015-CID361-9H

15 October 2015



Contact Information:

Cyber Criminal Intelligence Program
27130 Telegraph Road
Quantico, Virginia 22134

Phone: 571.305.4482 IDSN 2401
Fax: 571.305.4189 IDSN 2401

E-mail

CCIU Web Page

CID Cyber Lookout
On Point for the Army

DISTRIBUTION:

This document is authorized for wide release with no restrictions.



"DO WHAT HAS TO BE DONE"

Extortion Scams: Awareness and Reporting

Recent data breaches have exposed millions of records containing personally identifiable information (PII), personal health information (PHI), details of financial and brokerage accounts, and credit/debit card numbers and PINs. The [Identity Theft Resource Center](#), a U.S. non-profit organization tracking data breaches, reports that since 2005, more than 828 million records from more than 5,500 confirmed data breaches have been stolen. In the first nine months of 2015 alone, more than 175 million records were compromised in 591 data breaches.

If your data has been stolen, cyber criminals may target you with spam, phishing emails, threats of future exposure, promises of protection from future exposure, and identity theft and credit repair services. Be suspicious of communications regarding the data breaches that do not come from credible sources. It is likely a fraud or extortion scheme. Proceed with caution and VERIFY, VERIFY, VERIFY!

If you receive email you believe to be an extortion attempt or fraud scheme, take these measures:

- If the safety or wellbeing of someone is in imminent danger, contact your local law enforcement authority immediately!
- Do not reply to the email, click on any links or open any attachments
- Report the email to the [Internet Crime Complaint Center\(IC3\)](#)
- File a complaint with the [Federal Trade Commission](#)
- Report the email to your email and Internet service provider (ISP)
- Move the email to your SPAM folder
- If contacted through social media, report the contact to the social media provider as well

If a Soldier, Department of the Army Civilian, or someone affiliated with the Army is attempting to extort or defraud you, contact your installation Military Police or Criminal Investigation Command (CID) office. (Contact Info: [CID Locations CONUS](#), [CID Locations OCONUS](#), CID by email at Army.CID.Crime.Tips@mail.mil, or call 1-844-ARMY-CID (844-276-9243))

Additional Information

[Cyber Sexual Extortion](#), U.S. Army CID
[OPSEC on the Cyber Home Front](#), U.S. Army CID
[Online Misconduct: Awareness and Reporting](#), U.S. Army CID
[Credit Freeze FAQs](#), Federal Trade Commission
[Identity Theft Victim Resources](#), Identity Theft Resource Center
[How to Protect Yourself After a Data Breach](#), Market Watch

ICE

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

Disclaimer: The appearance of hyperlinks in this Crime Prevention Flyer (CPF), 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. Such links are provided consistent with the stated purpose of this CPF.