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

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

E-mail

CCIU Web Page

CID Cyber Lookout
On Point for the Army

"Do What Has To Be Done"

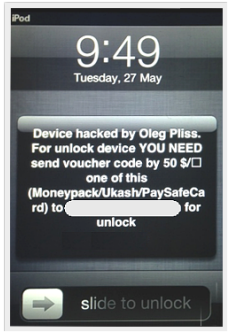
CPF 0016-14-CID361-9H **30 June 2014**

Apple Mobile Device Ransom Scam

Overview:

The purpose of this Cyber Crime Prevention Flyer is to inform all service members and Department of the Army civilian employees of a recent scam wherein two Russian cyber criminals were targeting Apple device (iPhone, iPad, iPod, and iMac) users and locking the device until a ransom was paid. First appearing in Australia and eventually in the U.S., the cyber criminals socially engineered Apple device users, via phishing emails and a fraudulent iCloud website, into providing their Apple ID and password. With the collected information, the cyber criminals logged into the device owner's iCloud account, put the device in "Lost Mode", locked the device with a pin, and commanded the devices to display a message demanding a $50 to $100 ransom be paid via an online money transfer service.

The individuals behind this recent phishing scam have since been arrested by Russian authorities. However, Apple devices make up a large percentage of the mobile device industry and it is highly likely cyber criminals will continue to target Apple devices and their owners.



Tips to Avoid being Socially Engineered via Phishing Emails:

- Be suspicious of unsolicited email messages from individuals and companies. If an individual claims to be from a legitimate organization, try to verify their identity with that organization.
- Do not use contact information provided in the email or on a website connected to the request.
- Do not respond to email solicitations.
- Do not follow links sent in email solicitations.
- Do not provide personal, financial, or account (username and password) information to email solicitations.
- Pay attention to the URL of a website in email solicitations. Malicious websites may look identical to a legitimate site, but the URL may use avariation in spelling or a different domain.

Cyber Crime Prevention Flyer

Apple Mobile Device Safety Tips:

- Use strong, unique passwords.
- Make sure your Apple mobile device has a passcode lock or Touch ID, fingerprint authentication, enabled.
- Activate the two-step verification for Apple ID
  - Two-step verification requires you to register one or more trusted devices you control that can receive 4-digit verification codes. Any time you sign in to your Apple ID from a new device, you'll need to verify your identity by entering both your password and a 4-digit verification code.
  - With two-step verification, you will also get a 14-digit Recovery Key to print and keep in a safe place. The Recovery Key can be used to regain access to your account if access to a device is ever lost or a password forgotten.
- If your Apple mobile device becomes locked and you receive a ransom message, do not pay the ransom. First contact your local law enformcement agency and then Apple at 1-800-275-2273 or through Apple's support site http://www.apple.com/support/contact/. You can also restore your device from a backup via iTunes or iCloud.
- Once you regain control of your device, change your Apple ID immediately.

Previous Related Cyber Crime Prevention Flyers and Cyber Crime Alert Notices:

Remote Hostile Takeover - Smartphone Security (16 Jan 2013)

Mobile Device Malware - Avoiding Mobile Device Malware (18 Oct 2012)

Held for Ransom - Ransomware (4 Sep 2012)

CCIU Cybercrime Advisories

Additional Advice:
U.S. CERT Tips
www.us-cert.gov/ncas/tips/

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

ICE

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

CCIU's "Toucan Lan" keeps an eye on cyber crime issues of interest to the Army community.