



COT Security Alert – Malicious Email Attachment

COT Security has received reports of state government email inboxes receiving spam emails that have malicious attachments. Some of the reports show users are forwarding the emails to others for assistance when they are unable to open the attachment.

Currently, the subject line on the malicious emails is “NCIJTF Security Policy” and the attachment is named “Questionnaire.docx.zip”.

End users are reminded to:

- **Never open attachments in suspicious emails**, even if they are from a known sender. The sender could be forwarding something harmful or may have unknowingly disclosed their credentials to malicious entities.
- **Never forward suspicious emails to other users.** Report them to the Commonwealth Service Desk (CommonwealthServiceDesk@ky.gov). A suspicious email is an email that cannot be verified to be legitimate and entices the recipient to take an action that could disclose confidential information (such as logon credentials) or which could harm their computer or the network.
- **Verify the purpose and intention of suspicious emails** that are from people you know by contacting them directly and **NOT** by replying directly to the email.
- **Never verify an email’s legitimacy using any information within the email itself**, such as by calling an included phone number.

A screenshot of the malicious email is shown below.



From: cywatch@ic.fbi.gov [mailto:skj-yasu@ii7.jp]
Sent: Monday, January 30, 2017 6:02 PM
To: |
Subject: NCIJTF Security Policy

According to *Appendix-1* to **The National Cyber Investigative Joint Task Force Policy Directive-29** all the public institution employees are to become familiar with the enclosed *Security Policy* document.

To become familiar with *The Security Policy*, please:

1. Unpack the 'securitypolicy.rar' archive in 'c:' directory.
2. Open the 'securitypolicy.docx' file.

If you have any questions, please contact **The NCIJTF Command Center** representatives (24/7)
Phone number: (855) 2923937
E-mail: cywatch@ic.fbi.gov

Notice: COT is providing this information so that you are aware of current security threats, vulnerabilities or preventive actions that may affect state government resources. If you suspect you have become victim to a security threat, please contact CommonwealthServiceDesk@ky.gov.

Confidentiality Statement - This communication contains information which is confidential. It is for the exclusive use of the intended recipient(s). If you are not the intended recipient(s), please note that any form of distribution, copying, forwarding or use of this communication or the information therein is strictly prohibited and may be unlawful. If you have received this communication in error, please return it to the sender, delete the communication and destroy any copies.

Office of the CISO
Commonwealth Office of Technology
Frankfort, KY 40601
<http://technology.ky.gov/CISO/>