Security Tips

NEWSLETTER

ETS
MCC EDUCATIONAL TECHNOLOGY SERVICES

Communications and
Network Services

Phishing Alerts - Fake Traffic Tickets & False Credit Union Messages

There have been a number of recent “phishing” campaigns, which are attempts by individuals or groups to solicit personal information from unsuspecting users by employing social engineering techniques. This month’s newsletter will focus on some of recent campaigns and provide guidance for protecting yourself and your information.

Did I just get a traffic ticket in my email?
State and local law enforcement organizations recently reported a phishing campaign in which individuals are receiving an email titled “Uniform Traffic Ticket,” and are informed that the attachment in the email is a copy of a traffic ticket. Users are instructed to fill out the attached ticket and send it to a town court. When a user opens the file attachment, malicious software (also called “malware”) is installed on their computer.
`

This attack relies on the concern that most individuals would have about receiving a traffic ticket. However, while most major law enforcement agencies may offer methods of paying a ticket online, we have no knowledge of any municipalities or entities that utilize email as the means of transmitting traffic tickets.

Why is the National Credit Union Association emailing me?
The National Credit Union Association (NCUA) reported that members of its credit unions are receiving emails with a variety of messages, purporting to be from the NCUA, asking recipients to click a link to another website. In this case, the link sends you to a website where you are asked to provide personal data, including social security numbers, passwords and personal identification numbers

The NCUA states: “It does not ask credit unions members for personal information. Anyone who receives a supposed e-mail or phone call from NCUA that asks for personal information should consider it a fraudulent attempt to obtain their personal account data for an illegal purpose and should not follow the instructions in the e-mail or phone call.” They further recommend that if you did respond and provided information, that you should notify your credit union immediately.

How can I protect myself?
While the above examples are only two of the many recent attacks, there are countless others, and new ones are being developed every day. Cyber criminals often exploit national and international newsworthy events. As we approach hurricane season and the 10-year anniversary of the September 11 attacks, we should be especially vigilant and

take precautions when receiving emails with links or attachments claiming to have event information or related details. Below are some guidelines to avoid becoming a phishing scam victim:

- Do not respond to unsolicited e-mails from unknown and untrusted sources.
- Do not open any attachments contained in suspicious emails.
- Do not respond to emails requesting personal information or that ask you to "verify your information" or to "confirm your user-id and password."
- Beware of emails that reference any consequences should you not "verify your information."
- Be cautious about all communications you receive including those purported to be from "trusted entities" and be careful when clicking links contained within those messages.
- If an email appears to be a phishing communication, do not respond. Delete it. You can also forward it to the Federal Trade Commission at spam@uce.gov or, in the case of the NCUA, to phishing@ncua.gov.

Resources for more information:

Internet/E-Mail Fraud Alert, National Credit Union Association:
www.ncua.gov/Resources/FraudAlert/Phishing.aspx

Uniform Traffic Ticket Hoax E-mail:
www.troopers.ny.gov/Public_Information/2011_News_Releases/08-17-11_UTT_Hoax_E-mail_Returns.cfm

FTC's Identity Theft Website:
www.ftc.gov/bcp/edu/microsites/idtheft

AntiPhishing Work Group:
www.antiphishing.org

OnGuard Online:
www.onguardonline.gov/phishing.html

For more monthly cyber security newsletter tips, visit: www.msisac.org/awareness/news/

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization’s end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization’s overall cyber security posture. This is especially critical if employees access their work network from their home computer.

Brought to you by:

MS-ISAC MULTI-STATE
Information Sharing
& Analysis Center™
A DIVISION OF CENTER FOR INTERNET SECURITY