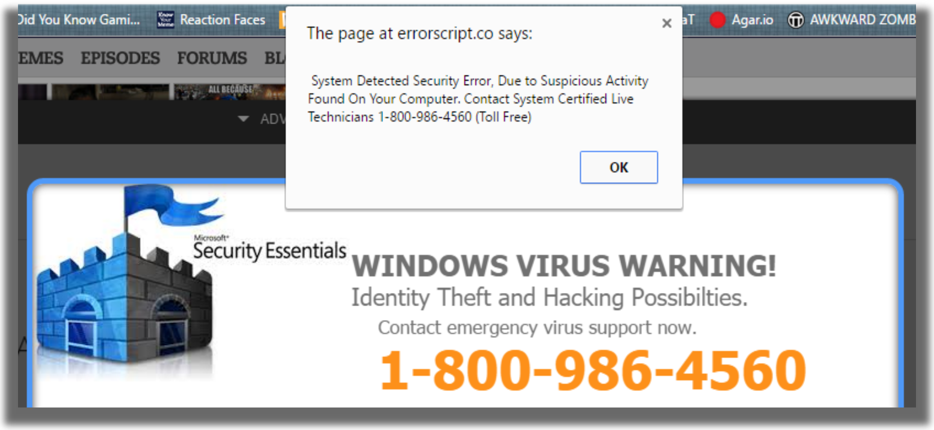
Week 1 – National Cybersecurity Awareness Month

Tech Support Scams

One of the biggest threats to our cyber security are tech support scams, including phone calls and pop-up ads on both phones and computers. These scams are a sophisticated form of social engineering—the use of deception to manipulate people into performing actions or divulging confidential or personal information.



The page at errorscript.co says:

System Detected Security Error, Due to Suspicious Activity Found On Your Computer. Contact System Certified Live Technicians 1-800-986-4560 (Toll Free)

WINDOWS VIRUS WARNING!

Identity Theft and Hacking Possibilties.

Contact emergency virus support now.

1-800-986-4560

Some scammers call and claim to be a company affiliated with Microsoft tech support. Other scammers send pop-up messages that warn about computer or phone problems. They say they've detected viruses or other malware and will ask you to give them remote access to your device. Eventually, they will diagnose a non-existent problem and ask you to pay for unnecessary – or even harmful – services.

If you get an unexpected pop-up, call, spam email or other urgent message about problems with your computer, stop. Don't click on any links, don't give control of your computer and don't provide any financial information or form of payment.

If you receive a phone call from someone you don't know it may be best to let the call go to voicemail. And don't rely on caller ID to prove who a caller is. Criminals can make caller ID seem like they're calling from a legitimate company or a local number. If the call is important, the person will leave you a message. That then gives you an opportunity to listen the message and make the best decision on how to respond.

If you're concerned about your computer, call the help desk directly at 1-800-373-7521 or email us at helpdesk@ssndcp.org