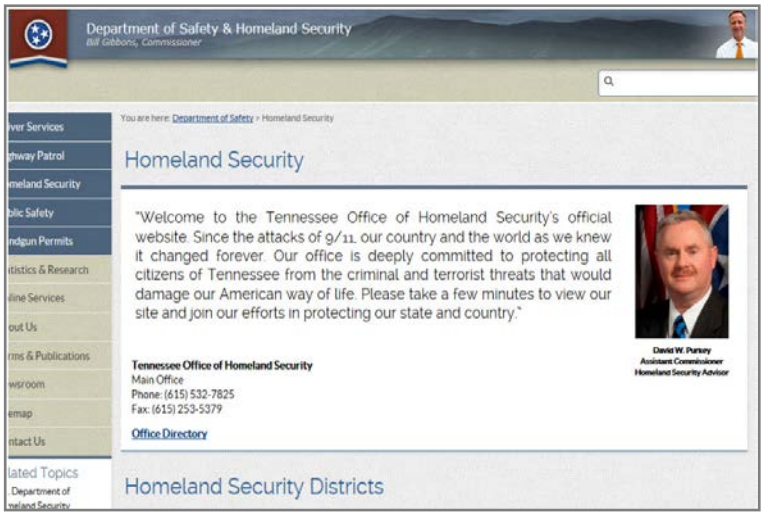
Impersonators Using Official State Website to Facilitate Online Scam

The Tennessee Department of Safety and Homeland Security (TDOSHS) is warning the public about criminals using publically available information from the official Tennessee Office of Homeland Security (TOHS) website to facilitate an online scam. The criminals have used both personnel information and photos in an attempt to make the fraudulent e-mails appear more legitimate. As part of the scam, the impersonator informs their victim in a series of e-mails of “Homeland Security” fees that need to be paid. If the victim refuses, the impersonator threatens that they will be arrested by Tennessee Homeland Security. E-mails from the impersonator may contain what appears to be the signature line of legitimate TOHS personnel or contain the Nigerian Economic and Financial Crimes Commission (EFCC) logo with a signature line of an individual claiming to be with the EFCC.

The public should be aware that TOHS does not contact members of the public demanding money or other forms of “Homeland Security” related fees. Anyone who has received an e-mail from an individual purporting to be with the TOHS demanding money should refuse the payment and immediately report the activity to the TOHS at http://tn.gov/homelandsecurity/report_susp_act.shtml .



Official TOHS State Website

EFCC Logo

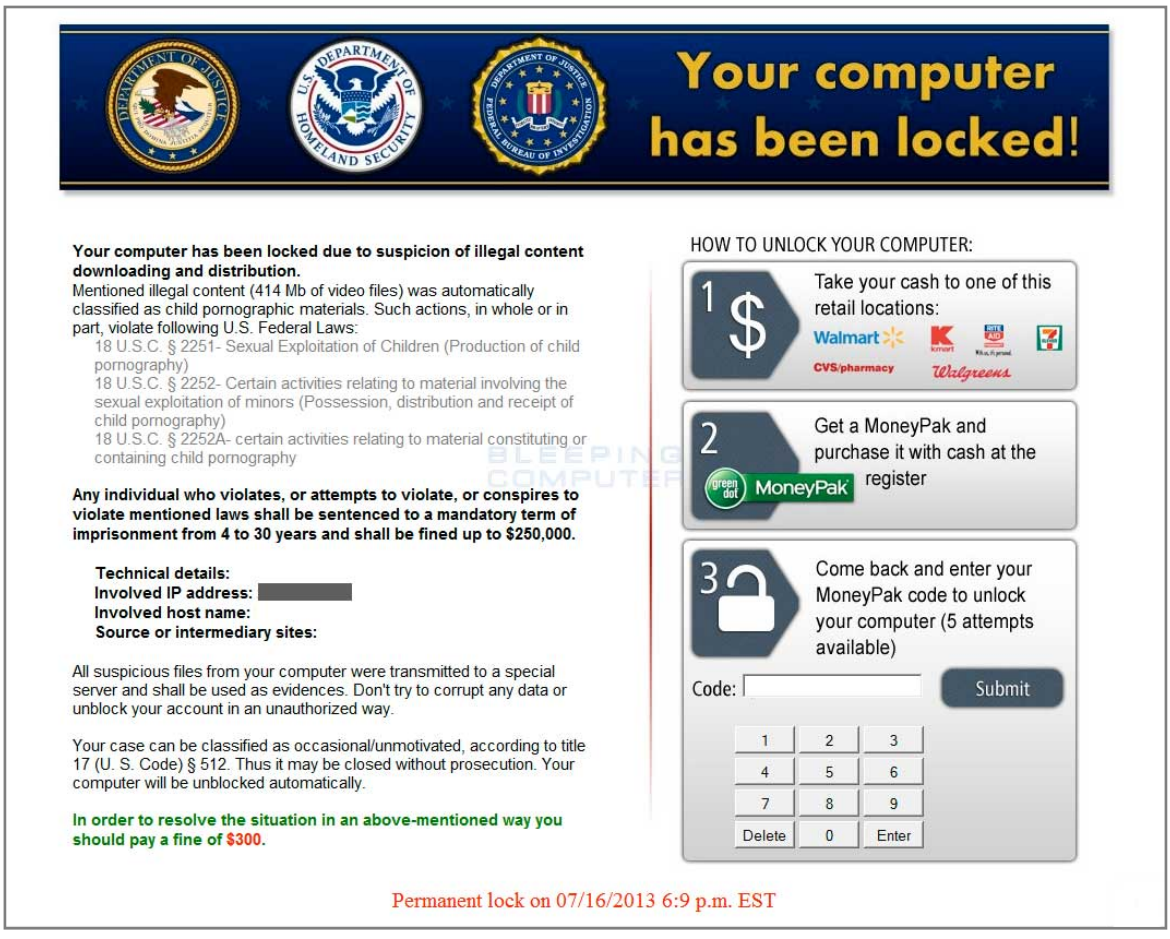
Other Schemes Recently Reported in Tennessee to TDOSHS

The TDOSHS would also like to raise public awareness of other schemes recently reported in Tennessee.

U.S. Department of Homeland Security (DHS) Themed Ransomware

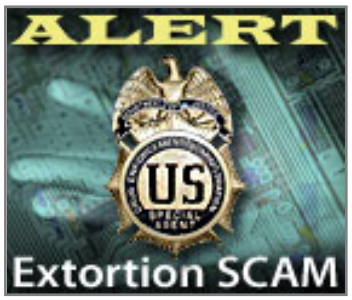
Individuals continue to report incidents involving the DHS themed Ransomware. Recipients of the ransomware receive a message advising the use of their computer is locked until a fine is paid. Recipients of this malware are encouraged to report the incident to the FBI at www.ic3.gov .

To remove the malware, the U.S. Computer Emergency Readiness Team (US-CERT) recommends consulting with a reputable security expert, or performing a clean reinstallation of the operating system after formatting the computer hard drive. Additional information related to this malware infection can be found at www.us-cert.gov .[1]



[1] (U) Recent Reports of DHS-Themed Ransomware, US-Cert, July 31, 2013, http://www.us-cert.gov/ncas/current-activity/2013/07/30/Recent-Reports-DHS-Themed-Ransomware-UPDATE

Drug Enforcement Administration (DEA) Extortion Scam



TDOSHS has also received reporting related to an identified DEA extortion scam. In a press release issued by the DEA, they are warning the public about the international scheme. In most cases, the criminals, posing as DEA special agents or other law enforcement personnel, target victims who have previously purchased drugs on the Internet or by telephone. The impersonators inform their victims that purchasing drugs online or by telephone is illegal, and that action will be taken against them until a fine is paid. Victims are instructed to pay the "fine" via a wire transfer to a designated location, most commonly overseas. If victims refuse, the impersonator often threatens to arrest them or search their property. Additional information related to this scam can be found at www.deadiversion.usdoj.gov/pubs/pressreleases.[2]

Phone Scam Targeting Knox County Restaurants

The Knoxville Utilities Board (KUB) is also warning of a scam targeting restaurants throughout Knox County. KUB became aware of the scam after being contacted by customers who received calls from individuals purporting to be with KUB advising of money owed on the account. To collect the money, the impersonator asks the customer to purchase MoneyPaks cash cards in specified amounts. Once the purchase is made, the customer is directed to provide the serial number on the card so the money can be collected. If the customer refuses, the impersonator threatens to cut off their power. KUB encourages individuals to contact them directly if they feel they have been targeted by the scam. Additional information related to this scam can be found at www.kub.org .[3]

The public is reminded to use caution if they receive unsolicited e-mails or phone calls demanding money or threatening enforcement action for non-compliance. Publically available information will continue to be exploited to facilitate various scams of this nature. Citizens are encouraged to continue to report suspicious activity to local law enforcement and the Tennessee Office of Homeland Security at www.tn.gov/homelandsecurity .

---

[2] (U) DEA Warns Public of Extortion Scam by DEA Special Agent Impersonators, DEA, Accessed on September 9, 2013, http://www.deadiversion.usdoj.gov/pubs/pressreleases/extortion_scam.htm

[3] (U) KUB Safety Alert-Scammers Targeting Locally Owned Restaurants, Knoxville Utilities Board, September 4, 2013, http://www.kub.org/wps/wcm/connect/9822d4b4-891c-40b4-881e-4ffc7f1224c8/Imposters+Alert+UPDATED+NR+-+9-4-13+FINAL+WEB.pdf?MOD=AJPERES&CACHEID=9822d4b4-891c-40b4-881e-4ffc7f1224c8