BCCS
Keeping You Connected

Telecommunications Bulletin

Customer Service Center (CSC)

Volume: CSC 13 - 06
September 21, 2012

Theresa Starling
Telecom Manager

Toll Fraud

Hackers with auto-dialers are a reality creating ever increasing toll fraud concern. This Bulletin outlines both proactive and reactionary measures that can be taken to minimize the risk. Under the terms of the state's current network contract, AT&T's Fraudulent Call Center provides NetPROTECT Basic Service, proactively monitoring all statewide voice lines for suspicious call activity. If AT&T detects suspicious calling patterns, the state site is contacted and AT&T places a block on the line(s) to prohibit international calling. If after internal investigation, the site contact determines the calls were legitimate, AT&T will remove the block upon request. If the calls are deemed fraudulent, the international block(s) can remain on the line(s). Regardless, the agency is responsible for the toll costs.

Phone systems (especially PBX/EKS systems with automated attendants or voicemail) are particularly vulnerable to hackers; thus, agencies should adopt "best practices" in regard to voicemail security at the system level. These practices include, but are not limited to, the following steps.

- Disable the remote notification and the call-outbound-transfer on temporarily unused mail boxes
- Lock voicemail boxes when users are on vacation or an extended leave
- Implement strong voicemail password management policies
    - Establish a minimum 7 digit password length,
    - Disallow repeating digits or a password that matches the voice mailbox number
    - Require password changes on a regular basis
- Delete all unused voicemail boxes immediately
- Consider requesting blocks to prevent international calling and the dial-around option (10-10 bypass) to select another long distance carrier

In addition to any lines blocked by the AT&T Fraudulent Call Center, additional lines at the location can, for no charge, have international calls blocked at the AT&T Long Distance level. However, this block does not prohibit a hacker from using the 10-10 dial around to other long distance carriers. POTS and business lines associated with a phone system can be blocked to prohibit both international calling and the 10-10 dial around. However, the Local Exchange Carrier (LEC) will charge for these blocks (charges vary by the LEC, but average $5.50 per line for both blocks). CMS is initiating a project in AT&T (Centrex) and Frontier (Centranet) areas to block 10-10 dial around and 411 (directory assistance) calling via Network Class of Service/Line Class Codes (NCOS/LCC). You will soon receive a separate Bulletin with specific details on that project's implementation.

Note: Centrex and POTS lines riding a PRI/T1 cannot be blocked at the LEC and restrictions can only be done at the phone system level.

As an added protection against toll fraud, AT&T NetPROTECT PLUS Service is available. In addition to the monitoring process, this plan provides an initial $2,000 liability cap in the event of reported fraud via the AT&T long distance network. If AT&T suspects fraudulent activity on a subscriber's line(s), they will place a block on international calling and contact the CSC so that we can engage the appropriate agency personnel. NetPROTECT PLUS has a $110 installation fee and an $11 monthly recurring cost

per location. (A location is defined as a single phone system or a single address with analog/digital phone sets supported by Centrex/Centranet.)

Customers subscribing to AT&T NetPROTECT PLUS Service will remain liable for all fraudulent usage charges incurred after the initial fraud notification until corrective action is taken and AT&T's fraud case is closed. After suspected fraud is reported, corrective action should be taken (as listed in this document). Then, after the location remains "fraud free" for 30 days, the customer liability cap is reset and increased by $2,000.00, resulting a new $4,000 cap. (Each time the liability cap is reset, it increases by $2,000.)

State offices that require international calling must be handled on a case-by-case basis. The CSC will consult with those offices and advise how to minimize phone fraud.

While all agencies should be proactive in minimizing their risk by taking steps before toll fraud occurs, the reality is that nothing can be guaranteed. Interested agencies should submit a Telecommunication Service Request (TSR) to establish blocks on POTS and business lines, create blocks at the system level, or subscribe to AT&T's NetPROTECT PLUS service. Send TSRs to the Customer Service Center, 120 West Jefferson, 2nd Floor, Springfield, IL 62702.

If you have any questions regarding this Bulletin's information, please contact Ed Fedor by email at Ed.Fedor@illinois.gov or at 217-524-9911.