July 13, 2016

Toll Fraud Cost Algona Businesses Money – Take Steps Now to Avoid Huge Long Distance Bills

TO: AMU Business Telephone and Internet Customers

Fraudulent activity can cost anywhere from $10,000 to upwards and beyond $100,000. Diligent security practices can help eliminate financial exposure. As a reminder, Algona Municipal Utilities recommends customers implement a variety of security measures to help identify fraudulent activity.

Start by eliminating surprises by becoming educated on current security threats. Next, establish and follow a security policy. Once you have a security policy in place, you'll want to secure your system configuration and establish a team to monitor security and service. Lastly, we encourage you to work with your equipment vendor.

Hackers use auto-dialers to search entire area codes to identify and target systems, regardless of where. They can identify the type of Key/PBX by the login procedure used for each system and know default pass codes for each vendor's PBX. Hackers also recognize the various voice mail systems by the default digitized voice recordings.

Typically, hackers can gain unauthorized access through the PBX's maintenance port, remotely accessed voice mail or the Direct Inward System Access (DISA) feature of a PBX. They'll call a customer's toll-free lines, use stolen calling cards and impersonate others to access your system. Hackers will use whatever means possible to illegally access your system.

While it can be difficult to stop hackers, your best defense is to be prepared. Below are a few recommendations you can incorporate to protect your business and customers.
- Contact your equipment vendor to discuss Key/PBX and voice mail security.
- Block operator services or international access as appropriate.
- Block casual dialing from the PBX: 01XXXX and 1010XXX.
- Change default passwords for users and administrators. Also, increase the length of passwords and restrict login attempts.

Other security measures to consider include:
- Deactivate unused features and voice mail accounts.
- Restrict message notification or out-dialing on voice mail boxes.
- Add verified account codes if international dialing is necessary.
- Review the call detail on monthly invoices and report anything suspicious.
- Invest in call accounting or station message detail recording software to review internal extensions for abnormal activity.
- Do not allow remote access until you are confident it is secure.

Having a properly secured telephone system is the best way to deter hackers. Be proactive and take the steps now to protect your business and customers. For additional assurance, Algona Municipal Utilities encourages you to consult your equipment vendor for assistance in securing your system security efforts.

Please contact me or any AMU Communications staff if you have any questions.

Sincerely,
John Bilsten, General Manager