NorthwesTel
Bringing us together.

An important message from Northwestel

Long Distance Fraud Warning Affecting Businesses with Owned PBX Systems

Northwestel has received recent reports of criminal activity, where customers are reporting being billed for long distance calls fraudulently made through their business voicemail equipment as known as PBX systems.

Below are the details:

The activity involves experienced criminals accessing unsecured business voicemail equipment via system option prompts that eventually permit the user to place long distance calls.

These criminals most often call a business after-hours and use its automated answering system to troll for vulnerable mailboxes. Experienced fraudsters sometimes recognize the equipment they are calling by its prompts and know the equipment's default passwords, allowing them access to mailboxes with unchanged passwords (or try guessing at simple passwords such as 1234 and 1111).

It is imperative for you to protect yourself against this type of fraud by ensuring your voicemail equipment is safeguarded and your employees are educated about password security best practices.

For customers with owned voicemail systems, you are responsible for the protection of your equipment and are responsible for any toll charges.

Industry best practices for protecting your voicemail equipment include:

- Ensuring your employees change the manufacturers' default password [immediately upon being assigned a voicemail box, and are trained to change the password frequently thereafter]
- Programming your voice mail system to require passwords with a minimum of 6 characters (8 is preferred – the more complex the password, the more difficult it is to guess)
- Training your employees not to use easily-guessed passwords such as their phone numbers, local number, or simple number combinations.
- When assigning a phone to your new employee, never make the temporary password the employee's telephone number
- Programming your voice mail system to force users to change their password at least every 90 days
- Validate if the through-dialling feature is needed, and if not it should be disabled by your equipment support provider. Through-dialling allows you to make long distance calls through your mailbox when you are at an offsite location. If this feature is used, it is important that you generate and monitor through-dialling reports to ensure your mailboxes are not being abused.
- Remove all unassigned mailboxes

The above security measures are of a general nature and might not protect every aspect of an individual telephone system – you are encouraged to contact your equipment support provider to discuss the unique aspects and vulnerabilities of your telephone equipment in greater detail. Remember that you are responsible for paying for all calls originating from, and charged calls accepted at, your telephone, regardless of who made or accepted them.

If you have general questions about voicemail equipment protection contact your equipment support provider.

Are you a victim?

If you suspect you have been a target of criminal activity, it is your responsibility to contact the local authorities immediately. Northwestel will be pleased to co-operate with you and assist in a formal criminal investigation with your consent and at the request of the RCMP.

Take steps to protect yourself

Today's sophisticated voicemail systems come with safeguards to prevent toll fraud. However, like locks on your car or on your house, they have to be used properly in order to be effective. Here is what you can do to increase protections for your business:

- Ensure that your employees change the manufacturers' default password immediately upon being assigned a voicemail box, and that they are reminded to change the password frequently thereafter.
- Program your voice mail system to require passwords with a minimum of 6 characters (8 is preferred – the more complex the password, the more difficult it is to guess).
- Train your employees not to use easily-guessed passwords such as their phone numbers, the number of their phone extension, or very simple number combinations.
- When assigning a phone to a new employee, never make the temporary password the employee's telephone number.
- Program your voice mail system to force users to change their password at least every 90 days.
- There is a feature called "through-dialling" that allows you to make long distance calls from within your mailbox when you are at an offsite location. Validate if the through-dialling feature is needed, and if not ask your equipment support provider to disable it.
- If you decide to keep through-dialling enabled, then it is important that you generate and monitor through-dialling reports to ensure your mailboxes are not being abused.
- Remove all unassigned mailboxes.

Possible features and recommendations that customers should be aware of relating to their specific system and Toll Fraud:

PBX

☑ Call forward external from end users phones should be restricted
☑ Redirect of incoming numbers to outside numbers should be restricted
☑ General Access phones should be limited to local calling only
☑ End User phone access levels should be assigned correctly for applicable long distance calling
☑ Access to known high toll fraud areas is restricted or limited using restriction tables
☑ Use of Long Distance Authorization Codes
☑ Monitor and track long distance activity using Call Detail Reports

Voice Mail

☑ Redirecting inbound calls via Auto Attendant to external numbers such as answering services etc
☑ Restrict or control Voicemail revert (0) – thru dialling to pagers and cells
☑ Restrict or control Voicemail Remote Notification to pagers and cells
☑ If available use Desktop messaging or remote notification to email to notify of voicemail messages
☑ End Users forced to change Mailbox access passwords on a regular
☑ End Users password minimum length is set at least to 6 digits or more
☑ Administration of mailboxes removing any unused mailboxes
☑ Restriction and Permission Lists are used to restrict outbound access where required

All Systems:

☑ Passwords should not be posted or distributed
☑ Passwords should be changed on a regular basis
☑ Passwords must be changed from default passwords
☑ Authorization codes should be changed regularly
☑ Restriction Permission controls should be in place to limit inbound/outbound transfers
☑ Monitor systems using traffic and call detail reports to check calling patterns

- calls to unusual locations
- high call volume
- long call durations
- international and calls to 809 or 900 area codes
- high traffic after business hours

If you have questions about voicemail equipment protection and have a Northwestel maintenance contract, contact a Northwestel representative. Customers can request an audit of their systems' current settings and configuration. The audit will provide a customer with knowledge of what their current system settings are but does not guarantee against the possibility of being affected by Toll Fraud. Any further work to implement changes recommended as a result of the audit will result in further fees billable over and above the Audit Fee.

For customers who do not have a Northwestel maintenance contract, please contact your equipment support provider.

For more information regarding Northwestel Policies or to address concerns you may have regarding Northwestel Policies, you may write to:

Northwestel Inc.
Attention: Regulatory Manager
PO Box 2727
Whitehorse YT
Y1A 4Y4
Telephone: 1-877-349-8222 (toll-free)