Vol. 5 No. 7
July 2013

BUSINESS insights

Why the simple password isn't simple anymore.

Businesses have always kept locks on their doors to keep out the local thieves. In today's digital world, however, businesses are threatened by people who could be on the other side of the globe.

The Internet makes all of our business operational, financial, customer information and communications data vulnerable. Hackers are not only after business and customer data, but many tap into phone systems and make hundreds of premium and international calls for free that then get charged to the business. Unfortunately, your business is responsible for those calls whether you made them or not.

Protect your business phones and data with a strong company password policy.
The simple use of passwords helps prevent these Internet threats to your network and your phone system, but the passwords themselves can't be simple anymore. That's because cyber criminals can now use sophisticated tools that can rapidly decipher simple passwords.

Therefore, it's critical for your business to establish a policy that you, your employees and your customers follow in the creation of voice mail and other system passwords to help prevent loss of important data and toll fraud from hacked telecom systems.

A strong business password policy is the best defense to help ensure that the passwords accessing your system are the least vulnerable. Here are the critical issues your business should follow in relation to establishing and managing passwords:

- Make sure employees create passwords to replace the default passwords that come with the voice mail and network systems.
- Never use the employee's telephone number as a temporary password when assigning a phone to a new employee.
- Immediately remove all unassigned mailboxes.
- Educate users on the best way to create passwords that are the hardest to break. Strong passwords are built following these guidelines:
    - o Use the first letter of the words in a phrase that means something to the user. This makes the password appear to be a stream of unrelated letters.
    - o Use 12 characters or longer (eight letters is no longer considered enough and some security experts recommend 15).
    - o Avoid the use of famous names, common words in any language, words spelled backwards or words that use common misspellings.
    - o Do not use numbers in normal sequences: 1234.
    - o Employ a mix of capital letters, lowercase letters, and symbols.
    - o Never use personal information such as name, birthday, anniversary, driver's license, passport number or other personal information.
    - o Use different passwords for each login.
    - o Don't login with a password on a computer or device that does not belong to you.

(continue pg. 2)

IDEACOM NETWORK
1-866-IDEACOM
(433-2266)
www.ideacom.org

BUSINESSinsights

- Build a password checker onto your system's password creation page. This will help your users determine if the password they are creating is a strong one.
- Establish how often you require your users to change their passwords. Experts recommend that it be every 45 to 90 days.
- Build in a password history so users cannot reuse old passwords.
- Prevent the use of three or more characters from the user's account name.
- Never post or distribute passwords.

Your password policy should be designed to help ensure that users choose strong passwords. Of course, passwords that have been compromised should be changed immediately.

For even stronger security, some companies have dispensed with passwords and have implemented security tokens or authentication tokens that change the login ID number every few minutes. Users use a personal identification number (PIN) and the login to access the company network, which is displayed on a small, easily carried key fob. Large companies are moving to other forms of identification, including iris scans and finger prints.

For most businesses, however, the password is still the primary path to security. So it's important to make sure you educate your users to make sure the password does the job it's designed to do.

IDEACOM NETWORK
1-866-IDEACOM
(433-2266)
www.ideacom.org