GlobileNet

White Paper

# How safe is your Voicemail?

## Ways to prevent a hack on your system and save you thousands.

Our voicemail systems save us time and money. However, some systems have been the victim of hack attacks – unauthorised use of the system that can result in hefty bills and an administration nightmare.

It is important to be aware of the possibility of hack attacks on your voicemail system and to gather insights into voicemail related attacks, so that you can be vigilant and ensure your system's security.

Recently, a client was the subject of a hack attack; we will use their scenario here to explain who pays, how it happens and what you can do about it.

### HOW IS A HACK PERPETRATED?

In this particular case, the client has allowed remote access to voicemail using 4 digit pin codes. Once logged in, the user has been able to make unrestricted calls through that interface as no 'Class of Restrictions' were applied to the facility (e.g. international and mobile calls are allowed).

Let's say the client has a 100 number range from 9999 1000 to 1099 and publishes 9999 1000 as their primary listed number (assume direct dialing is available if the end-user number is known). In most systems, a single number is allocated to voicemail for all users, for example, the number 99991099 is allocated for remote voicemail access.

Typically, a voicemail user calls 9999 1099 and is prompted to enter a pin number (or voicemail number) at which time the 4 digit code is entered and they are then prompted via a menu to do what they need to do.

This is how a hacker might go to work:

1. Target a company or school and look up the listed number.
2. Research the company or school; look at their website, see if they can find out how large the organisation is (number of employees/ students), whether they operate over the weekend, perhaps even call the main number and ask for information directly. They may even get the Director's extension.
3. Now the hacker has an idea of the number range (let's say it's a 100 user school so it possibly has a 200 number range). Out of business hours, they call all the numbers in the range until they get a prompt for remote voicemail access.
4. While calling, there are certain signatures that vendors equipment provide that may help a hacker identify the type of voice system used i.e. default music on hold is often a giveaway! Research the vendor and find out defaults – it might save a lot of time.
5. A 4 digit code can range from 0000 to 9999 – even manually the hacker could attempt a crude "brute force" attack by trying all numbers sequentially.
6. Now the hacker can make international calls – and if they are careful, they may never need to pay for an international call again. They'll use the system from 10.00PM on a Friday night and cease calling 4.00AM. You find out on the Monday when the carrier has called you and alerted you of unusual use. But it's too late.

### SO WHAT CAN YOU DO?

We install systems that are delivered to your specified requirements. For example, you may wish to have access to voicemail remotely and also wish to make calls through that connection i.e. pressing an option that calls that customer/caller back or being able to dial another number from that facility.

Specifying 'Class of Restrictions' on voicemail ports can restrict an attack to local and mobile dialed numbers. However, this is not to say it can prevent fraud only that the attacker needs to do more.

It may be best not to allow any calls to be made via the voicemail port – only use it as a collection point. Alternatively, use voicemail to email options that are available on modern systems.

In any event if it is not clear, providing any such facility like other electronic access, introduces the risk of unauthorised access (hacking) and the installer cannot guarantee that unauthorised access will not occur.

We suggest that a risk/benefit analysis would necessarily include the possible cost of unauthorised carrier costs (due to a hack attack) and the possibility of sensitive information (voicemail messages) being available to a successful hacker. Other risk (normally already considered) includes complete loss of the telephony system and its adverse affects on the company performance and what risk mitigation strategies to use.

**POLICY, POLICY, POLICY**
This implies that your school needs to have a communications policy that includes data and voice security requirements. The policy should include staff training requirements and restrictions on what can and cannot be done through any such facility. E.g. Does your school allow international calling by all employees? Do you allow remote access to voicemail and can calls be made via the remote access facility?

If you provide this policy to the installer and the installer agrees to install the system to meet that policy, then a duty of care exists on the installer to make sure the system meets that requirement i.e. if your policy says that remote voicemail must be accessed through a 4 digit pin sequence and that no calls can be made across that facility, the installer has a duty to set the system up that way. The installer generally will set pin codes to some sort of default as they will with system passwords.

Note also that pin codes do not need to be 4 digits only – it will depend on your brand of voice system. Some only allow 4 digit codes.

**STILL UNSURE?**
If you are unsure of how to check your security posture on this subject, please feel free to contact us on free@globilenet.com. We do offer a chargeable security audit service if you wish to engage us.

**WANT TO KNOW MORE?**
Nothing is safe so we encourage you to spend 10 minutes looking at the following web broadcast http://www.instructables.com/id/How-to-hack-a-voicemail-box-how-to-reset-your-v/ which relates to personal voicemail.

Just a note, we cannot accept responsibility for a clients security as we do not control the voice environment. Telstra also has made it clear they will not provide any protection to their clients although they provide some capability to inform a customer when dialing habits change dramatically.