Fraud Protection

Assisting you in protecting your business against phone hacking fraud

RPM SOLUTIONS

Jaime Roue reports on Fruad Prevention

If you'd like to know more about how to protect your business against fraudulent calls please call our specialist team on 0333 6006 999

Unfortunately, we live in a world where no telecommunications system is impenetrable and completely immune to threat of a hacking attack, however at RPM we take the matter very seriously and we are determined to help reduce the risk which our customers face to the threat of this type of Fraud from ever-increasingly sophisticated hackers.

In 2011 the Communications Fraud Control Association (CFCA) carried out a comprehensive worldwide communications industry survey that assesses global telecom fraud losses. They estimate Global Telecom Fraud to exceed $40 billion annually. This compares to Global Credit Card Fraud at just $7.6 billion!

To assist our customers against these hackers, RPM provide the following advice:

- Change all your passwords regularly and make sure they are not default passwords. This includes Network, Systems, Routers, Modems, and Computers.
- Ensure that every mailbox on your voicemail system has a secure password, not a default one.
- Disable all Conference facilities if you don't use this function, or regularly change the access code.
- Be aware that SIP trunks are susceptible via the public IP addresses attached to the Telephone System or your Computer network.
- Be aware that you are responsible for the security of your lines, your telephone systems and your Computer network and for any calls charged to your account as a result of hacking.
- Bank holidays and weekends are a favourite time for Hackers to try and access your systems.
- RPM do not block premium rate numbers automatically as many businesses use them for legitimate purposes, however, we will happily apply this bar at no extra cost

RPM's Support engineers are here to help should you require assistance if we maintain your telephone system.

If you are ever in the unfortunate circumstance of being hacked, RPM suggest:

1. Raise this with the police and get a Crime reference number
2. Check with your insurance if you have 'Cyber Liability' cover - this is relatively new but was launched to combat telecom fraud
3. Check with your IT provider that your networks are locked down
4. Check with your IT provider that there are no open ports on your router/firewall
5. Change your voicemail PIN's - RPM can assist you with this
6. Check if there has been any spurious calls into the office recently from unrecognised users trying to:

a. request a call transfer between personnel until they obtain an outside line/obscene phone calls,
b. continuous hanging up, recurring incidents of asking for an invalid extension, wrong numbers,
c. callers asking who they have reached and silent calls that wait for you to hang up.

7. Rationalise voice mail boxes to ensure personnel who have left, have had their mail box deleted - RPM can help with this if you advise us of any users

So what are we at RPM doing to assist you protect your business against this type of fraudulent activity? The answer is our 'CallGuard' product.

RPM's CallGuard specifically enables:

- Automatically cut off any phone number with usage of over £500.*

If your phone number spends more than £500 in 24 hours on traffic which is not UK geographic or UK mobile we will cut it off automatically (we can easily turn it on again).

- Guarantee the charge limit on any breaches*.

If the 24 hour threshold is breached, you will not be liable for usage above £500.

- Automated notification of any cut-off *.

In the event of any of your numbers being cut-off, we will send you an email to notify you that a block has been applied. We can then remove the block, if required.

I'm astonished at how little other communication providers seem to be doing to battle this criminal activity and how some don't see it as a responsibility to their customers to do what-ever technology allows to assist.

RPM's CallGuard protects as much as technology allows in today's communications sector, however, we continue to research and develop this technology to ensure our support continues to be as effective as it can be.