Commission for
Communications Regulation

19/12/2012

For immediate release

ComReg Media Release

Businesses at risk of losing thousands through their phones being hacked this Christmas

ComReg has been made aware of a spate of business phone systems being hacked in recent weeks.

In the last 4 months there have been 12 cases reported to ComReg by operators. In one recent case of hacking, calls to the value of €90,000 were made without the knowledge of the customer. This type of incident is of particular concern as we approach the festive season when many businesses will be closed over the holiday period and may not notice their phones making thousands of international calls automatically.

Earlier in the year one company had calls to the value of over €250,000 made through its phones as a result of a similar type of issue. While ComReg was able to intervene in respect of some of these calls, the outcome was that the company was still liable for over €100,000 to its operator.

The problem is that business phones, often known as PBXs, have features on them which if not correctly installed and protected can be used by unauthorised third parties to dial into the system and place calls through the system without the knowledge of the business. Also in many cases businesses use external parties to maintain their phone systems which means that external access to a PBX is required. PBXs have maintenance ports to enable these maintenance companies to dial in to the phones to diagnose problems. Unfortunately these access ports are sometimes left open and have either weak or default passwords which are known by and easily exploited by hackers.

In some cases the systems can be hacked through the phone extensions when hackers dial in and access the system through those lines using the extension password, often 0000, 1234 or the same number as the extension.

What can you do?

If your business uses a third party to maintain the phone systems consider disabling the remote access and only enable it when you need agreed work done. If your maintenance company has remote access make sure they use a strong password and disable any default passwords.

You should ensure all your phone extensions have strong passwords to avoid individual extensions being hacked. These passwords should not refer in any way to the extension number.

If access to premium rate calls is not required from your phones ask your operator if those numbers can be barred. If your business doesn't dial internationally, consider asking for these numbers to be barred also.

Phone systems are like computers and are essential tools for businesses. If your computer held your bank details or any other sensitive information you would ensure that strong passwords and limited access were in place. Remember that your phone system can also be used to take money from you and protect it appropriately.

If your phone is hacked you should ask your operator to contact ComReg urgently as we may be able to help, but immediate action is necessary as it is normally not possible to take action after a few weeks have passed from the date the calls are made. You should also report the matter to An Garda Siochána.

Take action now to protect your business from the risk of receiving a phone bill for tens of thousands of euro.

Notes to Editors

ComReg works with operators and other regulators internationally (especially in the EU) to combat misuse and fraud involving telephone numbers.

See for example BEREC consultation:

http://berec.europa.eu/eng/document_register/subject_matter/berec/public_consultations/?doc=979

ENDS

Issued By

Eoghan McCarthy, Public Affairs, ComReg

Phone: 01 804 9758 **Email: eoghan.mccarthy@comreg.ie**