Q&A

Common Questions About Voice Security

Cavendish
COMMUNICATIONS

What's telecom fraud and why should I be worried?

Telecom fraud is a growing global crime in which groups of phone system hackers around the world target private business phone systems anywhere and reprogram them without anyone knowing so that they can stream all of their illegal traffic through them any time they choose making massive income for themselves. But your carrier network will expect you to pay when you get the phone bill because you are responsible for calls made via your phone system and not your carrier. This bill could be 10-100 times higher than your usual phone bill and sometimes even a lot higher than this. Everyone is at risk and all phone systems need to be secured against this crime to protect you from potentially significant financial losses. We can provide this security for you.

How will I know if hackers are or have been in my PBX?

Even before any attacks occur, hackers will have been into your phone system already without you or anyone else knowing about it. They covertly access your phone system usually via the programming ports and/or your voicemail boxes because they know all the access codes no matter how many times these are changed—and then they configure it for their own use—even creating their own voicemail boxes which you or your phone system maintainer won't even know about or be able to detect. In effect they "groom" your PBX so that they can bring it into commission for their own call traffic any time they choose. Passwords , no matter how many times they're changed, can't and won't protect your phone system because hackers can crack these easily with readily available online password-cracking technology. So, if you're unfortunate enough to get attacked once, it doesn't mean that'll be it for you. Once your PBX is in their network, they'll attack you randomly and repeatedly until your phone system is secured against these attacks. If an attack occurs during working hours you'll know about it though. Your phone system will light up like a Christmas tree with all your lines/trunks in commission for hours even though no one in your office is using the phone system and this means no legitimate call traffic for your business, inbound or outbound, can flow while the illegal traffic streams through your PBX. Hackers however, usually attack after hours or over the weekend or on holidays when detection is least likely and the first you will know about it is when you get your phone bill.

So if I get attacked, who pays for the calls?

You will. Carriers take the view that you're responsible for all calls made from your phone system whether or not you or your staff made them and whether or not your carrier/ airtime provider has taken any steps to stop or block fraudulent calls.

“

Telecom fraud cost businesses globally £53.2 billion a year in unauthorised call traffic through private phone systems but businesses have to pay for these calls

Why doesn’t my carrier just write-off fraudulent call charges ?

All calls, whether legitimate or fraudulent, are made over a number of different inter-exchange carriers and each carrier must pay their portion of the calls handled by them. Your domestic carrier and airtime provider must pay for all calls made to international locations even if they’re fraudulent so they have to recover this cost.

Why is preventing this fraud my responsibility ?

PBXs are the most common vehicle hackers use for their crimes. Only you have access control over your phone system. You carrier doesn't and cannot have this sort of access or control. So you’re responsible not only for its security but also for all call charges incurred from it. Moreover, only you can identify which calls made from your phone system are legitimate and which are fraudulent. Your carrier simply can’t do this with any accuracy.

We’re a small business. Why would hackers attack us ?

Hackers use “war diallers” (sophisticated software) to search globally for unsecured phone systems to harvest for their own use. And this search is continuous. They don’t care how big or small your business is. No one is safe. Worst of all for you if you do get attacked, you’re probably less likely to be able to absorb the average loss incurred from a hacking event and this can range from £10,000 to £100,000 or more in a single attack.

Why isn’t my current PBX secure then?

The resident security in your PBX was enough to keep you secure in the past but not now. Hackers, like the criminals who create increasingly intelligent viruses and spies to invade PCs/data networks, are becoming cleverer all the time in ways to attack and invade your phone system and they can easily circumvent this security now.

How do I justify the expense of fraud protection if we’ve never been attacked ?

Just because you’ve never been attacked doesn't mean it won’t happen. Hackers attack anyone anywhere and at any time. And its random. In other words past performance is not an accurate indicator of present threat. Years ago the equipment, technology and the motivation to perpetrate this crime didn't exist—but it does now. It’s really important you and your staff understand the need to protect your business and especially your phone system from this fraud now and to take steps to prevent unauthorized access to it.

> “
>
> Globally, telecom fraud is more than five times larger in terms of financial losses than credit card fraud but the prevention is much more simple.

But I’ve been in business for years and never heard of this crime and I’ve never been hit so why should I bother?

Your house has probably never burned down and your PC/data network has probably never been hit with viruses or spies either but we bet you have your house insured and your PC/data network locked down with anti-malware and firewalls just in case. Your phone system is no different and it’s just as vulnerable now. So, it’s all about minimizing risk and installing automatic protection just in case. It’s no secret that criminals always focus on the easiest target and up until a few years ago this was PCs/data networks — and then credit cards. With the advent of anti-malware and firewalls for PCs/data networks and then banks tightening up the rules on credit card security, these crimes have decreased significantly so criminals target the next easiest option — private business phone systems — to fund their activities and these are usually terrorist organizations such as the Taliban and Al Qaeda. It’s not a coincidence that in the UK, credit card fraud has decreased in the last few years while toll fraud has increased so that it’s now five times greater than credit card fraud and that’s because one is now pretty much secured while the other isn’t. Previously phone systems didn't have to be because they weren’t targets. They’re very much so now and this is why it’s critical you’re secured now.

OK. So what can I do to protect my business from this fraud?

It’s all about risk management. The better informed you are; the better protected you’ll be. The only sure way to protect yourself from this particular and financially damaging crime is with automatic, always-on, active voice security like Control Phreak which won’t let hackers anywhere near your phone system. It’ll kill all malicious call traffic in milliseconds while allowing all of your legitimate call traffic to flow. This means there’ll be no nasty surprises when you get your phone bill. Hacking is a predictable disaster — but it’s equally so easily prevented. The risk of becoming a victim of this fraud is already really high and increasing rapidly all the time but only you can control whether you’re attacked or not. It’s much easier to prevent an attack than to try to recover your business from a hacking attack. Phreaking is a preventable crime.

So if I install voice security and I still get hit, who’s liable?

Security for your PBX is no different from security for your PC/data network. Because it can be completely customized to match your operating and security requirements, you’re in control of it all the time so that you keep yourself safe while allowing all of your legitimate call traffic to flow. Obviously no one other than you can control what happens once the system is installed but in 10 years of testing and installation, not a single hacking attack has succeeded at any site running voice security. Of course that’s not to say it won’t happen because if someone disconnects the software from your phone system or switches off the PC it runs on or some other event happens to deactivate it, of course you will not be protected. Fraud protection is about empowering you to take control of your own security because only you know how you want this to operate — just as you’re in control of securing your PCs and data from viruses and spies.

> “
>
> The risk of becoming a victim of telecom fraud is already really high and increasing rapidly all the time but only you can control whether you’re attacked or not. It’s much easier to prevent an attack than to try to recover your business from a telecom fraud attack. Telecom fraud is a predictable disaster but it’s equally preventable.

Thanks for telling me about the risk but I’ll take my chances.

It’s really hard to understand why you wouldn’t be prepared to connect any of your PCs/ laptops and other devices to your network without security protection and you wouldn’t leave your office without securing the windows and doors and without activating the security alarm, yet you’re now declining to secure one of your most valuable business assets which, if it’s a attacked, could hit you really hard financially — and much harder than if any of your other security is breached. An average phreaking attack will leave you with a phone bill 10-100 times higher than normal—and often even higher than this.

The remedy for this crime is affordable and easily managed leaving you in complete control of your phone system so that you are protected not only against external fraud but from internal fraud too.

Only you can control whether or not you make a damaging financial loss.

Cavendish
COMMUNICATIONS

Cavendish Communications Ltd,
Cavendish House, New Road, Newhaven, East Sussex, BN9 0ES
Email: enq@cavcoms.com **www.cavcoms.com** **Phone: 0800 206 2107**