
Hackers
& Hacking
AVG Business

Look out!

From spear phishing to social engineering and Trojan horses - the ways in which a computer or network can be hacked have some rather obscure and technical names. But what do these dramatic-sounding threats really mean to a small business, and how likely are they to occur?

Introduction

The first step in tackling a threat is to understand it. This guide will demystify global hacking phenomena and explain how local and small businesses can inform and prepare themselves.

Joanna Brace is Vice President of Marketing & Product Marketing, AVG Business. Her track record spans brand-building, product development and marketing strategy. She joined AVG from Skype.

The Internet is growing at a staggering rate. Devices proliferate, user numbers continue to surge and the means of connecting devices, data and applications with the users grow ever more complex.

With accelerating levels of technological integration comes the opportunity to live and work in new and exciting ways. But with that change come certain risks. The more means we have to be connected, the more devices we use, the more windows of opportunity there are for hackers.

Many small businesses assume a hacker won't be interested in their data, misguidedly believing that they'd be more interested in hacking larger corporations.

Sadly, the evidence shows otherwise with the FBI reporting[1] hackers cost the US economy $8bn in 2014. So what can businesses do to prevent those attacks or at least lessen their impact?

The answers are simpler than you might think. Surprisingly, the number one solution to reduce the chance of being hacked is to use a strong password!

But that's not all, there are plenty more protective measures that you and your business can undertake...

1 https://www.fbi.gov/news/news_blog/2014-ic3-annual-report

Who are they?

Hackers are mysterious and secretive and their motivations vary. Just as the Internet has opened up new frontiers for trade, so have hackers from all corners of the globe found ways to identify new international targets.

Anonymity is the primary modus operandi, no matter what the nationality of the hacker. Hackers in, say, Brazil, can anonymously run phishing operations targeting web users in Spain, the UK and the US as well as targeting their compatriots. And they have done so. Cybercrime is so hard to police because of this lack of geographical restriction.

Whatever else can be said about them, hackers are highly skilled and technically competent people to say the least - don't be fooled by the "geek" label; the vast majority of web users would not have the slightest idea how to hack into, say, NASA or even a standard e-commerce system. And while hackers have many and varied reasons for doing what they do, it's not quite so hard to understand who they target and why.

Don't be fooled by the "geek" label

Larger corporates have more financial resource to invest in defenses. Hackers are well aware of this. They then logically target the weaker links in the chain - the suppliers, so often an SMB.

The data that these SMB suppliers process is often extremely valuable, both to the SMB and to the client they are supplying. Hackers know this too.

Anonymously, and from international bases, hackers produce programs and software designed to scour the web hunting for those weak links, wherever they may be.

Hackers don't just want purely financial information, personal profiling data is highly valuable to them because it helps them acquire other account details later on as is corporate data relating to new product research and development.

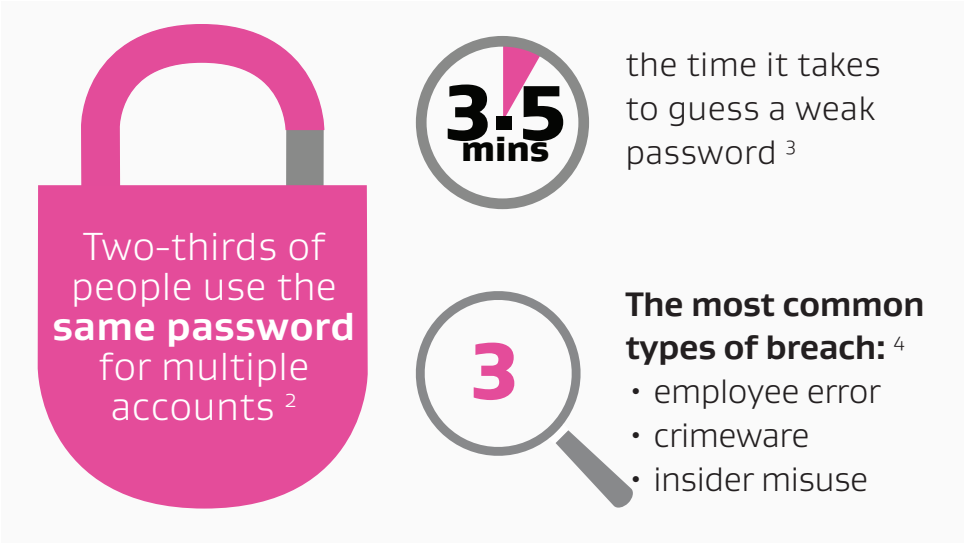
All too easy

The evidence is clear. Regardless of company size and regardless of the hacker's objective, the main reason so many smaller businesses are still hacked so easily is because of the low level security measures they have mistakenly in place. A shift in attitude is required.

What is not so clear is why businesses are still leaving their keys in the ignition. Believe it or not, the most popular password in 2014[1] was still 123456. Likewise, when a business owner thinks "I'm a small business, hackers won't be interested in me" they may not bother with higher levels of security. If they do, they're letting their guard down on at least two counts: a misguided belief and much weaker security, both of which increase the attraction and ease with which hackers can break in.

It doesn't take long to find a site or network with poor security either. Hackers don't spend days or weeks trawling the Internet looking for sites to hack, they create code to do that for them which ceaselessly scans for weaknesses, flaws and open doors.

A single hack may only result in a few hundred sets of credit card details, but that data is still highly desirable because of its value on the black market. Even if the hacker doesn't sell or share the data directly, they can use it to set up other accounts online and create false or duplicate identities based on real people - your customers - in order to commit fraud, other crimes or more simplistic disruptive activities.



1 http://arstechnica.com/security/2015/01/yes-123456-is-the-most-common-password-but-heres-why-thats-misleading/
2 http://www.entrepreneur.com/article/242208?linkId=14760815
3 https://blog.bit9.com/2015/03/15/dont-be-cracked-the-math-behind-good-online-passwords/
4 http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf

Be on guard

There are many ways to hack into a website or network - and it won't always be obvious that an attack has happened - but the most common forms of attack to look out for include:

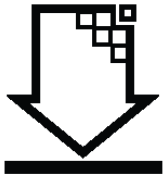
Phishing / Spear Phishing
Hackers will send you an official-looking email purporting to be from one of the sites or apps you might use e.g. PayPal. Or, it may appear to come from one of your own employees who occupies a position of high authority. In the email they will ask you to click on a link or reply to it with a certain piece of sensitive information.

Social Engineering
This is where a hacker attempts to gain the confidence of an authorized user of your website or business systems and gets them to reveal information that will enable them to later compromise its security. They might reach out to your employees on social media in and out of working hours or hang around a coffee shop near the office and strike up a leading conversation.

Cross-site Forgery
This is where a hacker tricks a legitimate user into giving out access details, usually by email or sending http requests, that will then enable them to exploit the computer or system e.g. modify firewall settings, post unauthorized data on a forum, or carry out fraudulent transactions.

SQL Injection
This is where the hacker adds Structured Query Language (SQL) code to a web form input box which then gives them access to your resources or the ability to make changes to the data in your systems. This kind of hack can go undetected and, in certain cases, seriously affect your search rankings.

Malware, Trojan Horses, Viruses, Worms, Spyware
These programs contain malicious code, sometimes hidden inside another apparently harmless looking program. When activated, they gain control of your computer and can delete or amend files, secretly capture your login details for other websites, or conduct other disruptive activities without you being aware.



Drive-by Downloads
This is where a person visits a web page and a piece of malware is downloaded without their knowledge or even deliberately clicking anything. That malware may then allow other types of hacking to take place.

Risk analysis

Capturing, storing and transmitting data through your business systems is a risk you can't avoid. But it is a risk you can manage. The greater risk is assuming you won't be a target because you think your business has nothing to offer a hacker.

You may not store any customer credit card details on your server, but your website can still be defaced or taken offline for other reasons. If that happens it could:

- **Stop orders coming through.**
- **Cause a loss of customer confidence in your site's security, brand or reputation.**
- **Cause customers to log on to a competitor's site.**

An emerging trend in the security industry is to think of your business as being in a constant state of compromise and flux.

This isn't as pessimistic or alarming as it sounds. It's actually more a pragmatic and realistically-minded recognition that, rather than trying to predict and defend against all possible attacks at all possible times (which is extremely resource intensive and costly), it is better to accept that a certain amount of compromise is always likely.

With that in mind, you can then maximise and allocate whatever resources are available in tackling the most virulent and prevalent attacks. This represents a constructive and helpful shift in attitude. It doesn't mean that small businesses accept defeat or ignore the risks; it means you accept that you can't always foresee every attack and instead you take steps to minimise the related impact.

In a short amount of time, by carrying out a few straightforward measures coupled with some fine-tuning, you can easily raise your level of security against the most common threats without it costing your business the earth. Take your time to consider them.

Protective steps

The best security policies start with the individual. If every staff member is well drilled in the subject of protective steps and security measures, the chain is immediately reinforced at every link.

The first thing you and your staff can do is to use a strong and unique password for each account.

The second important means of defense is to keep your passwords strong and confidential! You can put your business in a good position by:

- Limiting how many people have access to your systems.
- Limiting what types of data people can see and edit
- Changing the default password when you create an account
- Changing your passwords regularly, at least once a month is good
- Not using the same password for multiple accounts.
- Not writing down your passwords

Check Yourself!
Defeating or deterring the hackers doesn't stop at strong passwords. These simple checks will help ensure your IT security is in good shape:

Check your Firewall and AntiVirus
Are they both up to date? Are the right settings applied? Do this for every device in your network. Leave nothing out of date and no stone unturned.

A strong password consists of a mix of the following:

- Uppercase letters: F X W
- Lowercase letters: k g m
- Numbers: 7 4 9 0
- Symbols: @ & ! $
- 12 or more characters

Check your Backups
Running a daily backup means you can restore everything to a recent point in the past, limiting the loss and helping you recover as quickly as possible if you are hacked.

Check your Code
Assuming you do not have the appropriate internal resources, invite an IT professional to scan your systems and perform a penetration test to confirm that the coding and hosting of your website is both robust and free of common errors.

You may need to invest in an SSL certificate too but this isn't expensive.

But what if...

If you are unlucky enough to be hacked, knowing how to respond and what steps to take first could make all the difference. It proves to your customers that you are taking the problem seriously and reacting to their concerns and needs.

Focus
At this point you need to quickly understand what has happened, the impact it is having, the consequences, and how to fix it. This is not the time to go looking for a scapegoat, it is time for careful and considered action.

Be cautious
Don't dive in straight away and try to fix it yourself because you might make things worse, or disturb important evidence. Only fix it if you are absolutely certain you have the skills, tools, knowledge and authority.

Call in an expert
Yes it might cost you, but think of how much more it could cost if you cannot fix things quickly or in the right way: a loss of new sales, reputation, and loyal customers. Can you afford that?

Tell your customers
When you know what happened and how it affects your customers, tell them. Be open, upfront and honest. Your reputation is just as important as your sales. Ask them to change their password if they have an online account with you.

Upgrade and update
If you were hacked because of outdated software or hardware, this is the time to update and upgrade. If you were hacked because of outdated business processes, implement new ones.

Stay vigilant
Keep an eye open for news about the latest hacks, even if they happened to a large company or government. The same flaw may exist in your software, hardware, website or network. Find out what the cause was and figure out if it applies to you. If you're not sure, call in an expert.

How secure is your business? Click on the image above to use our SMB health check (see back page for full URL).

Go ahead

Hackers want what you don’t want them to have and will continue to look for ways to get hold of it. Whose will is the stronger and whose technology will falter first?

You don’t have to leave it to chance, you can improve your security and protect your business.

Learn more about internet security at www.avg.com/business-security
*** Small Business IT Security Health Check**
www.avg.com/small-business-it-security-healthcheck