# Don't Let Your Business Be Hacked

## The 6 biggest IT and cyber security risks for small businesses

USER ONE

# Contents

Contents....................................... 1
Introduction....................................... 2
1. Phishing....................................... 3
2. DDoS attacks....................................... 4
3. Internal attacks....................................... 5
4. Malware....................................... 6
5. Website vulnerabilities....................................... 7
6. Lack of education....................................... 8
Keeping your business safe....................................... 9

# Introduction

If you're a small business, it's likely you're already aware of the risks of hacking - but maybe you thought it would never happen to you. When it comes to your IT and cybersecurity, it's never been more important to keep up to date with how best to prevent risks for your business, keeping your customers safe, your data secure and your company protected.

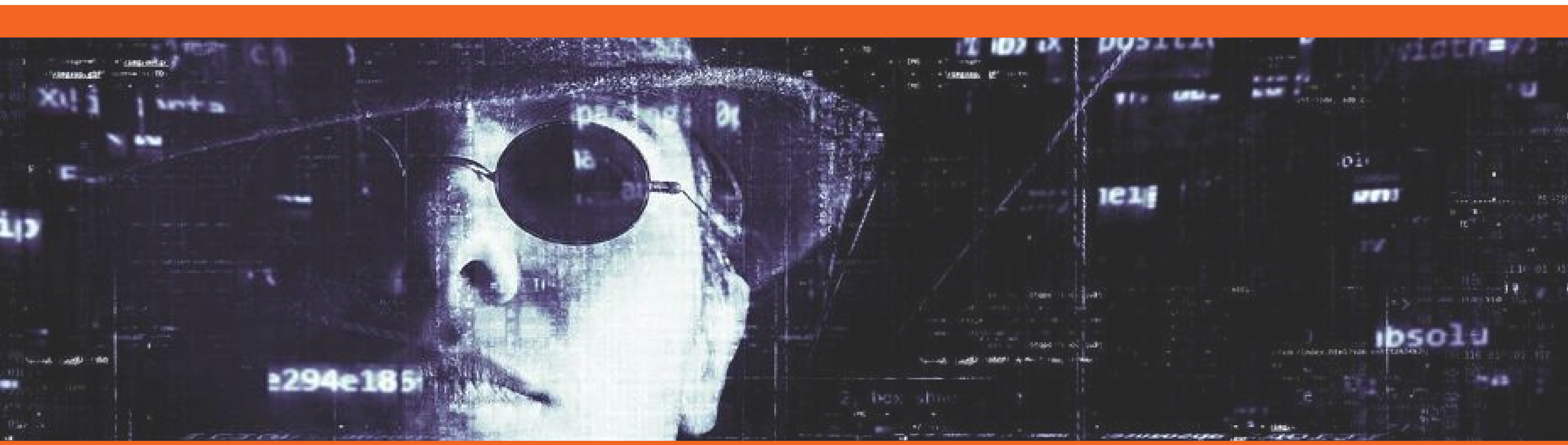
Read on for six of the most common causes of security breaches in small businesses - and a little information on the best ways you can prevent them from happening to you:

# 1 Phishing

Phishing can be a significant threat to small businesses, especially in companies that have less strict rules surrounding the use of email and communications. Phishing itself is characterised as malicious emails that reach out to the recipient to encourage them to click on a malicious link, which can then provide the phisher with access to all kinds of information and can even result in ransomware being placed on the computer. What makes these emails particularly hazardous is that they are specially formatted to appear genuine and look as if they have come from legitimate sources.

Even more dangerous is spear phishing, which takes the crime one step further: here, the phisher impersonates a specific person within the business to target their chosen victim. For an employee, an email may be perceived as coming from the CEO of a company, or their manager, and can sometimes be hard to discern at a glance.

It's crucial that employers make their staff aware of phishing, and ensure they make certain checks - like confirming email addresses and scrutinising the copy of an email - before clicking on any suspicious links, even for emails that seem to have been sent internally. There are tools available that can test your company's awareness and security when it comes to phishing emails which you can enquire about.



## 2 DDoS attacks

A severe and debilitating form of cyber attack, DDoS, or Distributed Denial of Service, is now a well-known part of the cyber landscape and has even been used to take down technology giants such as Twitter, Netflix and even Reddit with targeted attacks from dedicated hacker groups. DDoS attacks function by flooding a website or platform with a massive amount of views, users or visits, often resulting in the site being overwhelmed and having to temporarily shut down.

This type of attack is particularly problematic for any small business that primarily conducts its work online. DDoS attacks can be long and sustained, lasting up to multiple days and resulting not only in loss of revenue but also a lack of contact with clients and customers, such as through email or chat systems.

Though DDoS attacks cannot be prevented 100%, there are ways to reduce their impact or even prevent smaller attacks from affecting your business, by ensuring extra bandwidth is available at all times as well as having backups systems in place should the worst occur.

## 3 Internal attacks

Believe it or not, many cyber attacks don't come from elsewhere. In fact, internal threats are a grave risk to the integrity and security of your IT systems and online operations - especially with employees trusted enough to have access to highly sensitive data and information, or even access to specific systems beyond user functionality.

Depending on the sensitivity of your data, or people you work with as a small business, you may find that your employees are targets for bribery or even personal threats to access information. Or in other cases, they are happy to hand over information or login details to hackers or threats. Whether this is access to admin accounts, the passing on of information or providing a 'back door' to hackers, internal attacks can cause a great deal of damage in a short amount of time.

To reduce the threat of internal hacking or attacks, ensuring that employees are thoroughly vetted is critical. It's also essential to review access to valuable or sensitive information regularly. It's also vital to ensure that access is revoked immediately for anyone who leaves the company. This is to prevent unauthorised access further down the line.

# 4 Malware

There's more to malware than you might think. In fact, the title covers a variety of different malicious software and systems, all of which have the goal of accessing information in one way or another. Malware often goes hand-in-hand with phishing scams, though this is not always the case, and a variety of different malware types can infect your system.

Common forms of malware include ransomware, with which you are locked out of your system by hackers, often with a request for payment in cryptocurrency to regain access to your files and information. Spyware, adware and Trojan viruses and software are other common forms of malware, all of which can have a devastating effect on small businesses, from completely deleting your data to spamming your SEO, leading to your website losing its place in Google's search engine rankings.

Vigilance is key to preventing malware accessing your system, ensuring no suspicious websites are visited, or strange links clicked. Ensuring you have good quality antiviral software in place and backups of all your information that aren't connected to your central system are good ways to help defend yourself from these attacks.

# 5 Website vulnerabilities

When creating a website, often your primary focus is on how it looks and how it functions for your customers - but if you forget about properly securing your site against outside sources, you may be leaving yourself vulnerable to all kinds of attacks and problems. These are most commonly a result of outdated security or unprotected input forms, as a result of a 'weak point' in your code.

There are a variety of ways in which a 'weak' website can cause a problem for your business. Hackers may be able to utilise SQL Injection (SQLi) using unsecured forms through which they can gain access to your full database backend, which they can then use as they wish, leaving your customers also vulnerable to attack. This can then lead on to phishing scams, and negatively impact thousands of people from one little insecurity.

The obvious way to prevent vulnerability in a website is to always stay up-to-date with your security for your systems, especially with sites like Wordpress, where upgrading to the latest version is a must to prevent hackers from gaining access through security issues that have since been patched out.

## 6 Lack of education

It might seem obvious, but when it comes to your IT and cybersecurity, you may find that the number one cause of risk is the people who work for you. It's your responsibility as a business owner to provide your employees with the information, training and education to keep your business safe, which will also allow them to be safer in their personal lives when it comes to the use of IT and online systems.

Uneducated staff or those not taught to be wary of anything from suspicious phone calls to emails with unusual links are the most substantial risks to your business. Hackers require someone to click that link or answer those security questions in order to gain access to your system; without that first point of contact, it's likely that the majority of ransomware and viruses would be unable to access your network.

Providing formal training, simply sending reminder emails every so often or even providing a message at login can go a long way towards improving the vigilance of your employees, keeping your small business safer.

USER ONE

# Keeping your business safe

An educated business is a smart business - so remember all the risks that are out there next time you open a suspicious email or go to download something from an unsecured site. Keeping your small business safe can be as simple as being vigilant - but it's all about knowing the risks in the first place.

## Visit us

Unit 8 Foster Business Park
79 Boleness Road
Wisbech
Cambridgeshire
PE13 2XQ

## Follow us

f
G+ in

## Contact us

Telephone: 01945 463450
Email: info@userone.co.uk