CompuVision
Manage · Protect · Accelerate

Shut The Front Door

How individuals can leave the door open to hackers in an organization, and what you can do to secure your network

Contents

Introduction

We live and work in a world that is increasingly connected. Our personal and professional lives are dominated by digital tools and processes, and businesses are reliant on technology and online communication to grow and succeed.

Technology and the internet have changed the way organizations of every size do business, from startups to enterprise-level companies. Technology, innovation, and the digital world make our working lives easier, but there are risks involved too.

Almost every organization in the world uses digital tools and IT solutions in some form, from email to artificial intelligence. As businesses have innovated, so too have bad actors, and the vast amounts of data that are now available online can leave organizations vulnerable to hacks.

Cybercrime is nothing new. For as long as businesses have used technology to make work easier or faster, criminals have attempted to exploit weaknesses in it to gain an advantage. However, as tech becomes ever more advanced, and businesses migrate online in greater numbers than ever before, it becomes more of an issue.

Cybercriminals are often ahead of the curve when it comes to technological advances, and use increasingly subtle and nuanced methods to exploit vulnerabilities in our systems and networks.

From social engineering and ransomware to plain old human error, there are many ways that bad actors can gain access to your data, and steal information or money.

Luckily, businesses are not helpless in this! There are plenty of ways to protect yourself online, and plenty of habits, tools, and tactics that can boost your organization's cybersecurity and reduce the chances of a successful cyberattack.

This white paper presents 11 of the most common areas where businesses are most vulnerable, as well as some of the simplest and most straightforward ways that you can improve your cybersecurity right away. We hope it provides help and guidance in staying safe in an increasingly complex digital world.

Common Areas of Vulnerability

Password Security

Passwords are the obvious front door key to our accounts, networks, and systems. But all too often we are far more careless with these vital pieces of information than we ever would be with our physical keys. In fact, **30% of all successful ransomware exploitations happen because of weak passwords**.

Here are some of the key things to watch out for when it comes to password security.

Insecure or Publicly Kept Passwords

One of the most frequent errors people commit is not having a strong enough password. Whether it is the name of your puppy, the street where you were born, or god forbid, password123, easy-to-remember passwords are also easy to hack.

Secure passwords are a must. A combination of letters and numbers, upper case and lower case, with a sprinkling of special characters make for the strongest options.

But the most unhackable password in the world is of no use if it is prominently displayed on a post-it note behind your desk! Despite a general understanding of security risks, it is still all too common for workers to note down their passwords in physical form as a memory aid. All it takes is a lost notebook or an unfortunately angled webcam, and you might as well have shared your credentials on social media.

Using the Same Password

Remembering multiple passwords across a range of accounts can be challenging. In both our personal and our professional lives it is likely that we will log in to tens, if not hundreds of different accounts across the week. So it is understandable that users often reuse passwords, to help them remember and make life simpler.

However, using the same password across multiple accounts is a huge ‘Welcome’ sign to hackers and bad actors. For starters, it reduces the hurdles that cybercriminals have to overcome as if they crack one password, they have cracked them all. But more importantly, you will be using the same login credentials across networks with wildly different security measures. Your work systems might have cutting edge cybersecurity in place, but the charity you volunteer for or your local football team probably don’t, leaving your data vulnerable, and opening every door for would-be hackers.

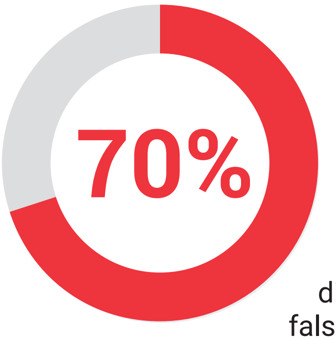
Shared Passwords

When collaborating on joint projects or accessing specific software with a single workplace license, it is not unusual for teammates to share passwords. When it comes to applications that a whole team needs to access, passwords are often stored centrally on a shared document, allowing everyone to have easy access.

However, if it is easy to access for your colleagues, it is probably just as easy to access for a hacker. All they need to do is get into an open, unprotected document, and they’ve slipped the lock to the front door and can begin to make their way through the system undetected and unimpeded.

Social Engineering

Social engineering is one of the most subtle methods that cybercriminals use to gain access to privileged information. It plays on human nature, manipulating, tricking, and controlling users to bypass security protocols, discover confidential data, and even take over your computer system. Social engineering can be carried out across all media – by phone, email, traditional mail, and even by face-to-face contact, and over **70% of all malicious breaches** are due to some form of social engineering.



> **People are used to having** a technology solution [but] social engineering bypasses all technologies, including firewalls. Technology is critical, but we have to look at people and processes. Social engineering is a form of hacking that uses influence tactics.
>
> – *Kevin Mitnick*

Phishing, ransomware, and CEO fraud are some of the most recognizable and dangerous social engineering methods in use at the moment.

Phishing

Phishing is when hackers and bad actors disguise themselves as trustworthy or known contacts in order to trick users into revealing confidential information like usernames, passwords, or credit card details. Phishing tends to use bulk emails, getting around spam filters and targeting users with messages from social media platforms, banks, or administrators.

Phishing is one of the most common and most effective form of social engineering. **More than 90% of successful data breaches begin with a phishing attack**.

Phishing attacks come in a variety of disguises, all designed to lull users into a false sense of security and trick them into revealing information they never normally would reveal. The top phishing techniques employed by bad actors are as follows.

Spear Phishing

While standard phishing attacks send large numbers of emails to as many recipients as they can, spear phishing campaigns are far more targeted and far more professional. Spear phishing targets specific individuals in an organization, and are usually aiming to acquire more valuable and sensitive data than just credit card details. Spear phishing attacks involve personal research on the targets, and are therefore usually more credible and successful.

Session Hijacking

Session hijacking attacks take over a user's web session by breaking into the control mechanism (using something called a session sniffer to access relevant server credentials), and steal data that the user shares during their session.

Email/Spam

The basic and most common type of phishing campaign sends spam email to thousands or millions of users asking them to provide various personal details in response to a false need or request. These messages are usually marked as 'URGENT', and often require the user to log in to an account to 'fix a problem', update information or verify details.

Content Injection

Content injection is particularly hard to guard against. With this form of attack, a phisher gains access to a trusted website, and changes part of the content (adding a link, or a form, or something similar). Users who are browsing legitimate websites are fooled into navigating away from the reliable pages, or entering personal details.

Web-based Delivery

Web-based delivery is immensely sophisticated, difficult to detect, and hard to guard against. In a web-based delivery attack the hacker gains access to a trusted website and locates themself between the website itself and a payment system. They are then able to track details of any transactions that pass through, without either the customer or the vendor being aware.

Link Manipulation

Link manipulation involves replacing genuine links with fake websites, and redirecting users to unsecure sites. These can be avoided by always running the mouse over a link before clicking it, and checking that the destination address is the expected one.

Malware

Malware is software that users accidentally download that allows phishers to take a variety of actions or record activity. Malware is usually installed when the user clicks a dangerous link, but sometimes arrives as an attachment to an email.

Keyloggers

A key logger installs a malware program that records everything that is inputted via a keyboard and transmits the information to a bad actor elsewhere. Hackers can then decipher personal details, passwords, and financial information from your keystrokes.

Smishing

Smishing is a portmanteau word used to describe phishing attacks conducted over text messages (SMS).

Trojan

A Trojan Horse is a form of malware that imitates a standard, safe action, and looks and acts like a legitimate program. However it really grants access to a user's account, allowing hackers to collect any stored information or infiltrate a network.

Malvertising

Malvertising is script contained within suspect or compromised web adverts that automatically downloads malware onto your computer or mobile device.

Website Forgery

Website forgery is the creation of false websites designed to look identical to the real sites they are imitating. These websites fool users into carrying out actions, making purchases, or entering details as if they were browsing a secure, verifiable site.

Evil Twin WiFi

A particularly tricky phishing scam, this sets up an unsecured wifi network, usually under a trusted name (Telus or TBayTel for example). Users logged on to this network will be sharing all information with bad actors elsewhere.

Ransomware

Ransomware is really a form of malware, but deserves its own section due to the devastating impact of ransomware attacks, and its increasing popularity among cybercriminals. By the end of 2021 it is estimated that the damage costs associated with ransomware attacks will be **over $20 billion**, and at present a ransomware attack against a company somewhere occurs **every 14 seconds**.

Ransomware attacks a system by encrypting it, locking users out of physical devices or making it impossible to access data. The hackers then demand a ransom in order to unlock the system, often within a certain time period before the data is destroyed.

Ransomware is damaging to organizations not just because they risk losing data or intellectual property, but also because it disrupts the smooth running of a business and causes downtime. This is why around 55% of small businesses who experience an attack pay the ransom rather than risk losing information and wasting valuable time. In some industries, however, a ransomware attack is thought of as a data breach, which can be crippling.

Ransomware gains access to a network via a phishing attack, through a dodgy link or compromised attachment. Once downloaded, ransomware will encrypt hardware, software, and any networks that it can access through the breached machine.

As a result, a single computer that is compromised with ransomware can bring an entire company to its knees. Businesses once were able to rely on data backups to avoid paying ransoms, as a full reset would restore the system and evict the hackers. But newer variants and strains of ransomware these days tend to target and corrupt backups as well. Around 34% of businesses don't test their backups on a regular basis, and a recent survey by Microsoft found that 42% of attempted recoveries in the last year were unsuccessful.

Ransomware attacks often involve an element of extortion, where hackers threaten to share confidential and sensitive information publicly if a ransom is not paid. In these cases the ransom might have to be paid twice, once to decrypt the system and once to delete the stolen data.

As mentioned earlier, the biggest impact of a ransomware is often not the data loss itself, but the downtime and cost of restoration. This has a particularly devastating effect on public institutions such as schools, police districts, and health organizations.

CEO Fraud

CEO fraud or business email compromise is an attack that disguises itself as a message or communication from the CEO of the organization (or other member of senior management) in order to trick employees into making unauthorized financial transactions or disseminating sensitive information.

CEO fraud includes domain spoofing, where hackers create an email address that mimics that of the CEO and sends messages requesting information or to transfer money, as well as traditional phishing attacks (spear phishing and 'executive whaling'). It also utilizes more sophisticated technology to go as far as imitating an individual's voice and carrying out fraud over the phone (known as 'vishing').

The FBI describes CEO fraud as "a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds."

CEO fraud is hugely profitable, costing companies over **$26 billion**. Instances of CEO fraud have been increasing dramatically over the last few years (an increase of 100% in global losses between May 2018 and June 2019).

CEO fraud tends to target HR, Finance, IT, and other members of the C-Suite. Hackers leverage time-pressured situations and large, sensitive deals where the CEO has overall signoff. Internal processes are often vulnerable when the CEO has final say, usually by email or phone.

Network issues

Of course, without a secure network with up-to-date and well-followed processes, vigilance and cybersecurity measures are useless. Problems with the network can leave organizations extremely vulnerable to attack, and can negate many of the good practices that businesses put in place to protect themselves.

Lack of Updates

A failure to install the proper patches at an individual and company-wide level can have devastating consequences. Software vulnerabilities come along all too often, and if you are working with out-of-date versions you are opening yourself up to a breach.

It is vital to update software immediately, and install all relevant patches as soon as they become available.

Poor Initial Setup

If your servers were set up poorly or carelessly to begin with, you may find you have backdoors and vulnerabilities in your system that you aren't even aware of. Server passwords, for example, are often left as default for the admin to change later on, but communication breaks down and they remain as '1234' or 'qwerty'. This allows bad actors to get in to the system at the ground floor with no one the wiser.

No Sandbox

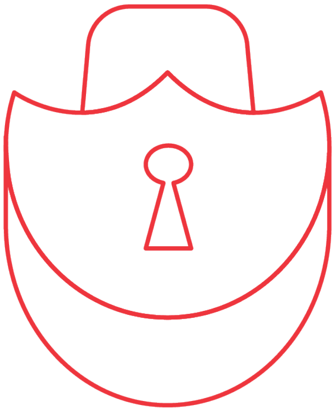
Any operating system or internet browser worth its salt these days should be designed to include sandboxes - areas that separate sections of the system from one another. These act like literal sandboxes, so that when malicious software penetrates one part of the network, it is prevented from spreading. Strict networks limit users' rights and privileges in order to maintain this structure, but if these limitations are not adhered to malware can go from being a contained nuisance to a devastating wildfire very quickly.

How to Protect Your Business

Cybersecurity can sometimes seem overwhelming. As cybercriminals use increasingly sophisticated technologies and ever more complex, nuanced methods, protecting yourself and your business from hacks, breaches, and vulnerabilities can feel like you are constantly playing catch-up.

But securing your network doesn't have to be a Herculean task!

While hackers, phishers, ransomware gangs, and bad actors are always on the lookout for vulnerabilities and areas of weakness, the solutions to these issues are often simple. So much of cybercrime comes down to basic human instinct, carelessness, or just lack of knowledge, and this can be addressed quite easily.



The feeling in the cybersecurity community is that organizations should consider it a case of when, not if they will experience a cyberattack. So ensuring that you, your employees, and your organizational and IT processes are fully prepared is vital.

Employee Awareness and Training

Ensuring that your employees know what to look out for, how to guard against the most common forms of cyberattack, and what to do if they encounter something dodgy is one of the most fundamental ways to protect your business against bad actors.

The vast majority of successful hacks and attacks involve some form of social engineering, and proper awareness and training can prevent many, if not most of these. The prevalence of social engineering attacks can lead organizations to view their staff as a liability when it comes to cybersecurity, but in reality you should treat them as the first line of defence, a human firewall. Equip your staff with the right tools, resources, and knowledge, and you give your organization one more layer of protection.

Security awareness training seeks to upskill employees to be able to better protect themselves and the company they work for from online threats. It teaches good digital hygiene, instills best practices in members of your team, and provides examples of suspicious behaviors to look out for.

Changing employee behavior involves a recognition that just educating your staff isn't enough. Exposing employees to information relating to cybersecurity is all very well, but for the process to be truly useful you need to involve in-depth training and systemic attack simulations and testing, so your staff know exactly what to look for, what to avoid, and what to do in problematic situations.

Updates and Patches

After social engineering attacks and phishing campaigns, hacks that focus on out-of-date and unpatched software are the most common, responsible for 20% to 40% of all data breaches.

Carrying out regular updates and patching vulnerabilities in your software is a huge part of maintaining a secure network, and something which needs to be a responsibility of every member of your organization, not just the IT team.

Of course, no one can patch everything perfectly all the time. There are tens of thousands of publicly announced vulnerabilities that need fixing, and however perfect your IT team is, it is not possible to stay on top of all of them.

But you can impress on your workforce the importance of not delaying system updates. CompuVision clients should remind staff to reboot their PCs at least once a week, to allow the installation of patches and updates to be completed in a timely fashion.

If you aren't a CompuVision client then aiming to patch better, not more, and to prioritize the most important updates will help you keep on top of vulnerabilities.

There are a few key best practices to keep in mind. Firstly, prioritize vulnerabilities that are released alongside public exploit codes. Those without exploit codes in the public domain are far, far less likely to be exploited, and can safely be dealt with at a later date.

Secondly, target the most important and most vulnerable software for patching. Internet browsers, OS, and Remote Desktop Protocols are the priorities on workstations, while web servers, databases, and 'listening' services accessible from the internet are the software most in need of updates on servers.

If you concentrate on dealing with vulnerabilities in these software programs first, you'll be able to cut out the majority of attacks.

Multi-factor Authentication

Multi-factor authentication is a great way to tighten up your password security and can do wonders to prevent issues that arise due to careless password management. Multi-factor authentication (MFA) requires users to provide more than one proof of identity in order to log in to an account, rather than just a password.

This might be additional security details (mother's maiden name etc), a security code sent by SMS, an additional authorization step using a device such as biometrics, or a physical 'key' in the form of a USB drive or similar.

Despite its reputation, MFA is not completely foolproof, and is still vulnerable to various phishing and social engineering attacks. But it is a vastly more secure way to protect your network and goes a long way towards dealing with some of the uniquely human vulnerabilities of any company. Its success and effectiveness is demonstrated by its use by companies like Google, Microsoft, Facebook, and Twitter, who have reported great results defending against the most common hacks by moving their customers from single-factor authentication to MFA.

Adopting MFA won't make your business impregnable, and it is vital to ensure that everyone in the organization understands that all other security measures, protocols and best practices still need to be followed. But MFA solutions do have the potential to make a big difference, and should absolutely be put in place.

AI Cybersecurity

Just as hackers are constantly innovating and experimenting with new technology, cybersecurity solutions are always looking to leverage the latest technology to protect organizations more effectively. Artificial intelligence (AI) is the latest and potentially most exciting development in this area.

Analyzing threats and improving cybersecurity these days often needs to take place in real time, and it is just not a human-level problem anymore. AI tools are now critical in facing the varied threats that bad actors can throw at networks, and more importantly, in predicting and preventing attacks from happening in the first place.

AI is able to analyze a huge amount of activity and identify vulnerabilities and threats far faster than human employees could ever hope to. This is vital when it comes to preventing malware from exploiting zero-day vulnerabilities, but can also learn and identify risky or suspicious behavior, and prevent threats or areas of weakness from ever becoming an issue. By analyzing vast amounts of data, both internal and external, they can detect and respond to anything out of the ordinary in real time, as well as predicting potential new attacks.

AI can help organizations manage their vulnerabilities, optimize and monitor data centers, and learn about normal traffic activity to maintain and manage overall network security.

Conclusion

Keeping your employees safe and protected is one of the most important aspects of a modern business. Protection from cybercrime is an exponential issue that businesses face everyday, and ensuring that your organization is as secure as it can be is vital.

Your front door should be shut, locked, and bolted.

With the rise of technology in the workplace, breaches and security incidents are on the rise as well. Businesses are traditionally focused on growth and can miss the protections needed to ensure cyber safety within their organization.

Our experts at CompuVision can create an affordable custom-fit information security package that suits your unique business needs. Whether you have existing in-house IT or are looking to move to managed services, our Protect+ offering is something no organization should go without.

With Protect+ our experts can create a custom-fit information security package that suits your business without breaking the bank.

Products like Ethical Phishing Testing and Advanced Threat Protection help protect your employees and create a culture of security awareness, while also making sure best practices are being followed.

Dark Web and Live Network Monitoring give us early warning indicators a security breach may be on the horizon and help us protect your network quickly if a threat is discovered.

Protect Plus secures, educates and prevents, allowing you to focus on what you're best at – running your business. We will take care of protecting your employees, preventing threats, and promoting awareness.

Contact Us

Questions?

Get in touch and let us know how we can help. With offices in Edmonton and Calgary and local representation across Canada and North America, we have someone nearby ready to answer your questions.

General Inquiries and Sales: 1-587-525-7600

Email: info@compuvision.biz

CompuVision Systems

Edmonton, Canada

Suite 101, 15511 – 123 Avenue NW
Edmonton, Alberta T5V 0C3

Calgary, Canada

Suite 355, 3115 – 12 Street NE
Calgary, Alberta T2E 7J2

Houston, United States

Suite 105, 21830 Kingsland Blvd
Katy, Texas 77450

CompuVision

Manage • Protect • Accelerate