# 5 Top Cybersecurity Threats & Solutions for 2020

STRAIGHT EDGE TECHNOLOGY

## Our world lives, works, and plays on the internet.

The internet links our cars, homes, infrastructure, and even home appliances.

And while the internet increases our connectivity and efficiency, it also brings a threat:

Cyber hacking and the need for cybersecurity.

According to Norton Security, nearly 60 million Americans have been affected by identity theft.  In 2023, it is estimated that cybercriminals will be stealing 33 billion records per year.

These cyberattacks target everyone, but trends show small businesses are one of the most common targets.  In 2019, approximately 43% of cyberattacks targeted small businesses.

Thankfully there are programs and safety measures available to help protect you and your business from cybercriminals.

Straight Edge Technology has identified 5 of the top cybersecurity threats for 2020 for small businesses and what you can do to prevent them.

This E-book covers a brief history of cybersecurity, four common cybersecurity threats, and Straight Edge Technology's top five cybersecurity threats for 2020.

Are you ready to learn how to equip your business with proper cybersecurity for 2020 and beyond?

**Let's get started!**

# Table of Contents

1. A Brief History of Cybersecurity
2. Malware
3. Ransomware
4. Social Engineering
5. Phishing
6. Top 5 Cybersecurity Threats in 2020

*Phishing*

*Malware & Ransomware*

*Database Exposure*

*Credential Stuffing*

*Accidental Sharing*

# 1

# A Brief History of Cybersecurity

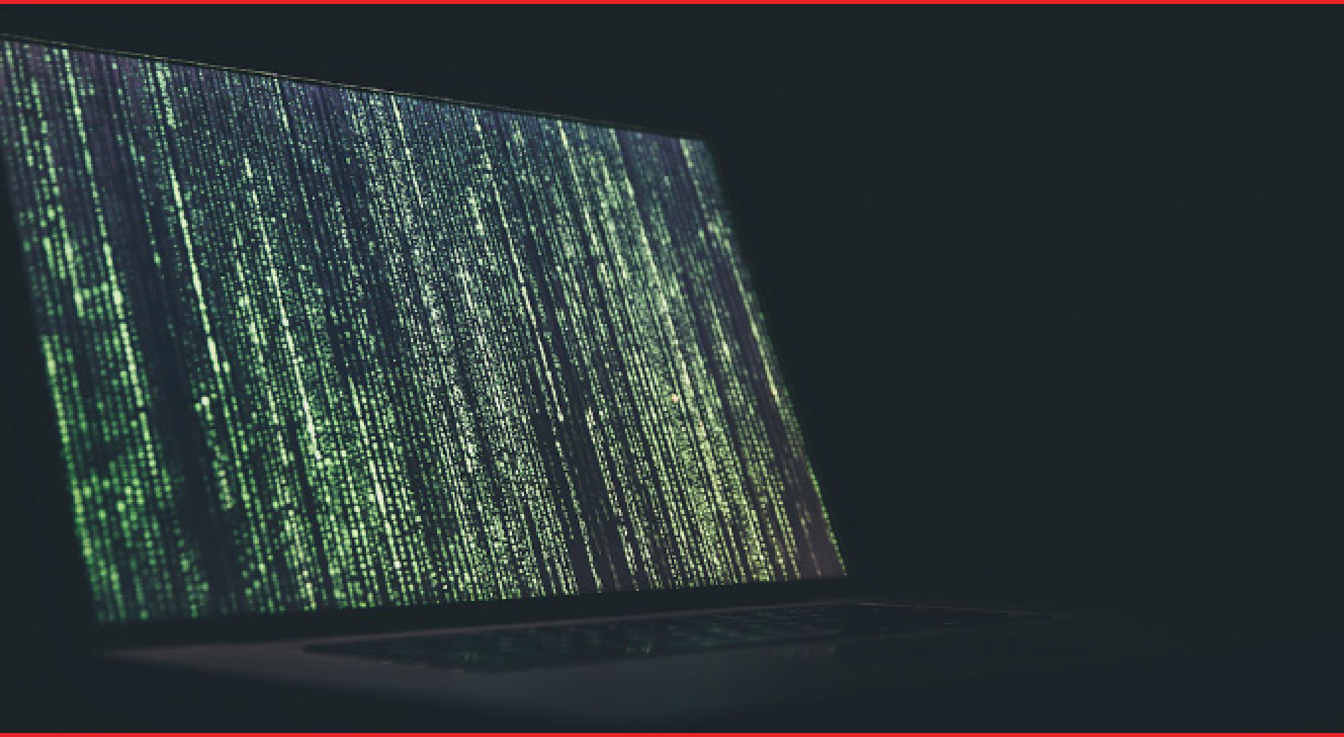
Cybersecurity is a buzzword, and people have different definitions in mind when discussing it.

In its most basic form, cybersecurity is “the protection of computer systems from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.”

This definition brings out two aspects of cybersecurity not often considered.

First, very few people think of the hardware or physical computer components when they think of cybersecurity. In today’s world, cybersecurity is associated with internet and software attacks.

Second, cybersecurity was a threat before the internet. As long as there have been computers storing data, thieves have been trying to steal it. While this was more difficult before the internet, it did occur.



## First Cyberattacks

*When did the first cyberattack occur?*

Believe it or not, one of the first cyberattacks was more of a game, not an attack!

In 1971, Bob Thomas developed a computer program able to travel between connected computers.

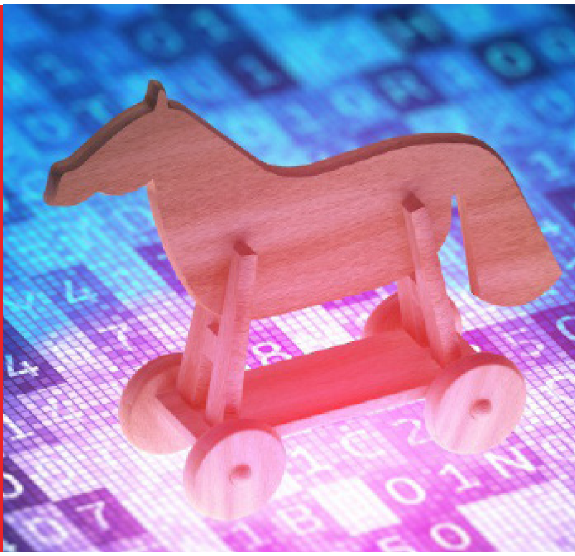
His program did no damage. Instead, it displayed a message stating, *"I'm the creeper: catch me if you can."*

As the internet became more widespread, many people didn't understand the risks of having connected data and computers with little cyber protection. This was not a significant concern since few malicious programs existed.

*When did this begin to change?*

In 1989, Joseph Popp created one of the first malicious computer attacks. He created a malware program called the "AIDS Trojan."

Initially passed by a floppy disk, the program was poorly designed and did not disable the computer. The main thing it did was scramble the names of the files. Programmers corrected this problem quickly with computer software designed to combat the AIDS Trojan.



There was another cyberattack in 1989, but this one was not programmed to be malicious. Instead, the creator wanted to raise awareness.

Robert Morris was concerned by how much data was easily accessible on the internet. He saw how much of this data was poorly protected by flawed security and weak passwords.

To show people how vulnerable the current security was, Morris developed a computer worm that significantly slowed down the internet.

While the worm was programmed to prove a point and do no actual damage, estimates say it cost between $100,000 and $10,000,000 from lost productivity, unstable internet, and restarting IT systems.

## Cybersecurity today

In today's world, cybersecurity is a part of life.

With virtually everything connected online, cybersecurity has never been more critical.

Sadly, it is still common to hear stories of data breaches. Banks, credit card companies, online retailers, phone companies, and others have had their customer's data breached and stolen.

Thankfully there are many companies actively developing better cybersecurity programs. Companies like Microsoft, Apple, and Google are constantly updating the software used on computers, servers, tablets, phones, and other devices.

The U.S. government also knows the importance of having proper cybersecurity, and in 2019 it expects to pay around $15 billion to protect its data. The Department of Defense uses over half of this budget, while Homeland Security comes up second.

So, what are some of the most common cyberattacks? While many exist, let's look at four common threats.

## 2

## Malware

Malware is one of the broadest terms when it comes to cyberattacks. It is any malicious form of software designed to harm a computer system.

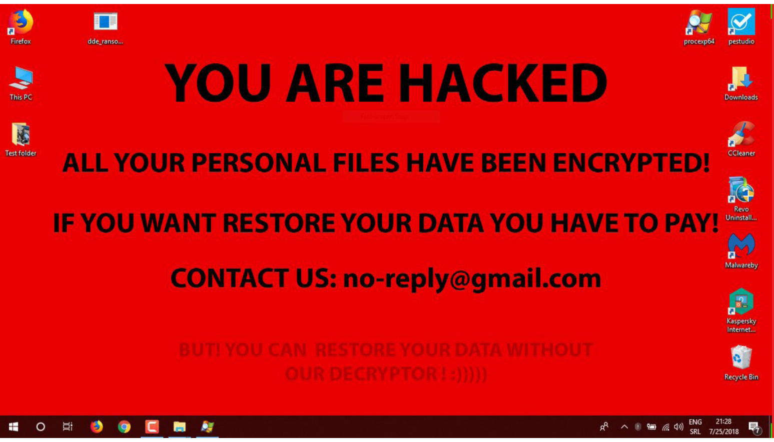
Malware includes worms, viruses, Trojan horses, and spyware.

Malware is designed to steal, encrypt, or delete data, alter or hijack core computer functions, or track a computer user's activity without their knowledge.

Malware is commonly distributed through physical drives, like a USB or external hard drive, or through internet downloads.

# 3

## Ransomware



YOU ARE HACKED

ALL YOUR PERSONAL FILES HAVE BEEN ENCRYPTED!

IF YOU WANT RESTORE YOUR DATA YOU HAVE TO PAY!

CONTACT US: no-reply@gmail.com

BUT! YOU CAN RESTORE YOUR DATA WITHOUT OUR DECRYPTOR ! :)))))

As the name indicates, ransomware involves the hacker locking the victim's computer or files and holding this information for ransom. It typically requires the victim to produce a payment before these files and system are unlocked.

Ransomware spreads through phishing emails or unknowingly visiting an infected website.

Ransomware is devastating due to the difficulty in recovering affected data.  While some victims do choose to pay the ransom, there is no guarantee the hacker will give control of the computer or files back to the victim.

# 4

## Social Engineering

Social engineering attacks rely on human or social interaction. Some reports estimate 93% of business data breaches came from employees unknowingly engaging a social engineering attack.

Social engineering attacks occur when a hacker tricks someone to give them information or access to software or data. Hackers try to manipulate people into breaking standard security procedures.

*What tactics do hackers use in social engineering?*

Because it relies on social interaction, social engineering attacks usually play on a person's emotions.

One of the most common tactics is to have someone think they are helping someone in need. For example, an attacker may pose as a fellow employee or a family member asking for access to a document, bank account, or sensitive data.

Social engineering is different from malware or ransomware because of the human interaction it uses. Properly built IT systems help prevent malware attacks, but they cannot stop an employee from giving a password to a hacker posing as a coworker.

*So how do companies combat social engineering attacks?*

Many companies have regular training for employees on how to spot social engineering attacks and strategies.

It is also important for businesses to have guidelines in place when working with sensitive data.  For example, a common rule is not allowing employees to share company usernames or passwords electronically.  If an employee forgets a password, they should call a coworker instead of emailing them.

## 5

## Phishing

While it is a social engineering attack, phishing has become one of today's most common and malevolent cybersecurity attacks.

In its most basic form, phishing occurs when a hacker uses a false identity to trick someone into providing sensitive information, downloading malware, or visiting a site containing malware.

*What makes phishing so prevalent in today's world?*

The extensive use of electronic communication; including email, text messaging, instant messaging, and social media accounts.

A common phishing tactic targets people through email. An attacker might create an email looking like it comes from your local bank, and the email asks you to visit a website and enter your banking login and password.

Another common tactic is creating a fake social media account resembling a friend or family member. The hacker then asks for money or data through messaging, and it appears it is your family member or friend asking for a favor.

*What can be done to protect from phishing?*

Like any social engineering attack, having training and guidelines in place is a crucial first step. People can be trained to look for specific phishing patterns and tactics.

It is also important to know how businesses will contact you in regards to sensitive information. Emails asking for bank information is a common phishing tactic, and yet most banks tell their clients they will never email them asking for their information.

If you receive a sensitive request from a business or a direct message from a social media friend, you should contact the company or person directly to see if the request is legitimate.

# 6

# Top 5 Cybersecurity Threats in 2020

Now that we have some background on what a cyberattack is and some common attacks, let’s focus on what this means for a small business.

As a small business owner or employee, you know how important your security and data are.  Even if you have an IT service provider, it is still good to have some knowledge of the technology threats your business faces.

Straight Edge Technology provides IT services and network security in the San Antonio and Corpus Christi areas, and we know how important your security is to you and your company.

Following are the top 5 cybersecurity threats Straight Edge Technology sees for local businesses in 2020.  Solutions are provided that your company can implement to reduce your risk and exposure to these attacks.

Some of these threats and their solutions are basic, and others are complex.  Working with a managed IT service company will help protect your business from these threats.  Even if your company has an IT department, it is recommended that you consult an outside IT company to make sure you have maximum security.

*Are you ready to be more confident entering 2020?*

*All right, let’s get started!*

*Threat 1*

## Phishing

As mentioned before, phishing is becoming one of the most common cyberattacks due to the high levels of interaction humans have on electronic communication.

In business offices, Straight Edge Technology sees this becoming even more of a threat as email and IM communication increase.

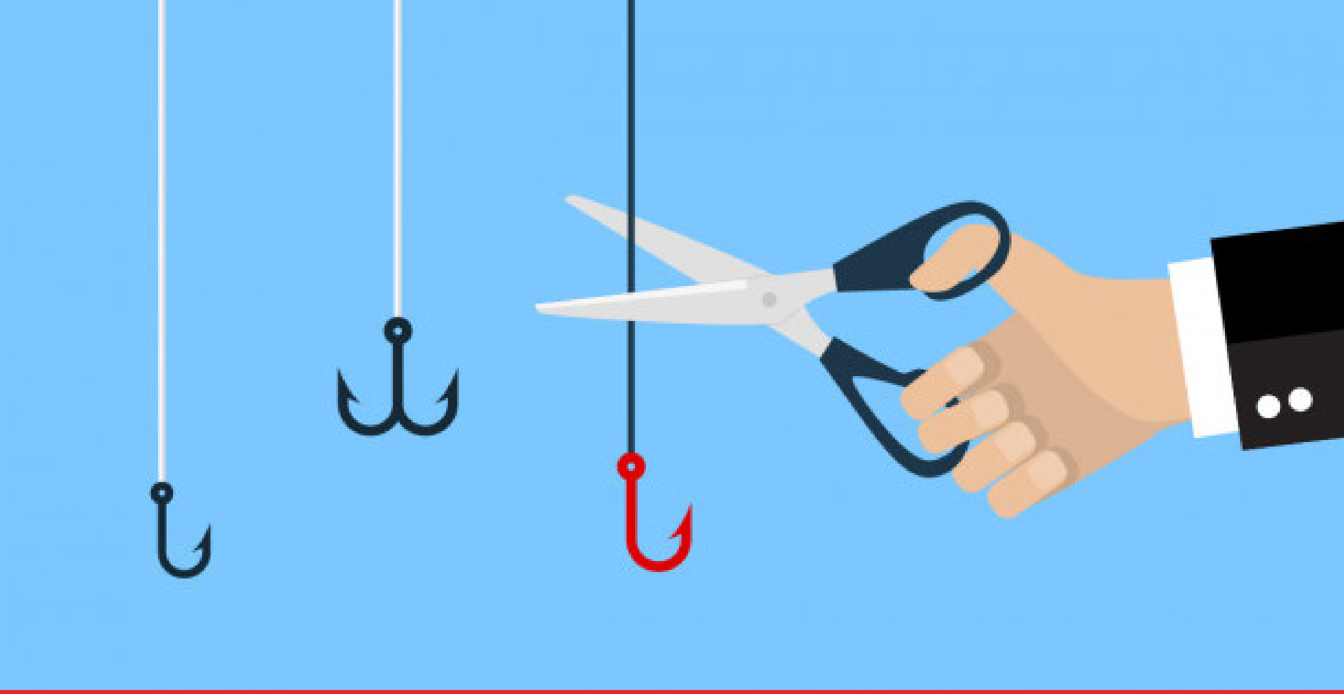
Office employees receive hundreds of emails and electronic messages every day. Towards the end of the workday, as minds become tired, humans are susceptible to making bad decisions if they are tired or overworked.

Attackers know this, and they continue to bombard employees with fake emails and social media accounts.  After all, a hacker can destroy a business's integrity with only one employee making a mistake.

This happened earlier in 2019 to Carle Foundation Hospital.

Through a phishing scam, hackers gained access to three of the employee's email accounts.  In the ensuing investigation,  it was determined these accounts gave the hackers access to sensitive patient medical records and Social Security information.

Thankfully the hospital reached out to affected patients.  It also recognized the need for more training in their employees.



## *What should your company do to protect itself from phishing?*

***First,*** watch for unusual emails and instant messages. They may start with unusual wording such as "Dear Customer" instead of using your name, and they often have a generic signature.

***Second,*** be cautious in clicking links or giving sensitive information, even if it appears to be legitimate. If in doubt, directly contact the source to make sure they sent the message.

***And third,*** install anti-phishing toolbars on internet browsers. These toolbars alert you to sites containing phishing information.

## *Threat 2*
## Malware and Ransomware

We already discussed the devastating impact malware and ransomware have when they infect a computer system.  Lost data, frozen systems, and hijacked software are just a few of the problems.

Although not based on social interactions, Straight Edge Technology still views them as highly prevalent in 2020, especially in small businesses.  Knowing many companies keep their data on servers connected to the internet, hackers are continually attempting to hack existing IT solutions.

Sadly, Pitney Bowes Inc. experienced this first hand.

Pitney Bowes Inc. helps small businesses with e-commerce, shipping logistics, and mailing services.

Earlier in 2019, they became a victim of a malware attack that encrypted information on some of their systems and affected customer's ability to access their services.

Although there was no evidence customer records had been stolen, the malware crippled the company's services. Customers were not able to upload transactions, access their accounts, or refill their postage.

When they realized they had been attacked, Pitney Bowes Inc. immediately had their technical team assess and fix the situation. They also brought in 3rd-party IT consultants to prevent future attacks.

## What should your company do to protect itself from malware and ransomware?

***First,*** make sure you keep all your computer software and hardware updated.  Outdated software, drivers, and other plugins are common security vulnerabilities. If you have an IT service provider, check with them to make sure this is happening on your servers as well.

***Second,*** enable click-to-play plugins that keep Flash or Java from running unless you click a link.  This reduces the risk of running malware programs with Flash or Java.

***And third,*** removing old software, sometimes referred to as Legacy Apps, reduces risk.  For example, if you are running Windows 10, but you run programs designed for Windows 7, then these are Legacy Apps and may be a security risk. Your software company should be able to give you an updated program designed for Windows 10.

*Threat 3*

## Database Exposure

Database exposure is what it sounds like: Due to a security breach, database information is exposed to hacking or theft.

Database exposure occurs in a variety of ways. Hackers might be able to steal login credentials through social engineering or use malware to gain access.

Because most companies use servers to host customer information, Straight Edge Technology sees database exposure being a big concern in 2020. These databases include customer contact information, financial records, or identity records such as Social Security numbers.

One of the significant issues with database exposure is that it becomes fuel for social engineering attacks.

For example, let's assume a company has a database exposure that releases names, email addresses, and birthdates. Using this information, a hacker could fake the identity of a local hospital and send each person an email with their name and birthdate. These people will be more likely to open a link in the email because it includes personal information and appears to be a legitimate email from the hospital.

Recently around 250,000 American and British job seekers had personal information exposed when two recruitment sites, Authentic Jobs and Sonic Jobs, failed to set their cloud databases as private.

As a result, personal information, including phone numbers, email addresses, driver licenses, and salary expectations, were made public.

It is unknown how much of this information was harvested by hackers, but it provided a gold mine of personal data for potential social engineering cyberattacks.

After learning about the exposure, the companies immediately made their databases private.

## What should your company do to protect itself from database exposure?

***First,*** if you have a private server, keep the physical hardware in a secure and locked room.  This helps prevent theft if your building is robbed, and it keeps unauthorized personnel from accessing it with a portable hard drive.

***Second,*** make sure you have a database firewall and web application firewall. A locked door protects your physical server and hardware, and firewalls protect your server on the  internet.

***Third,*** keep access to the server limited.  Each person with a login to the server is a potential leak, so the fewer logins the better.

***And fourth,*** encrypt the data on the server and keep a regular backup.

*Threat 4*

## Credential Stuffing

Credential stuffing is an attack geared toward stealing user access through login credentials.  This is most common in situations where the same login credentials are used for multiple sites or accounts.

With most programs being either online or connected to the internet, Straight Edge Technology expects credential stuffing will be a major threat in 2020.

Canada Post, the postal operator in Canada, recently discovered some of their users' account information had been hacked in 2017 by credential stuffing.

Although the exact number of affected accounts was unknown, Canada Post immediately began resetting all their user's passwords.

While investigating the incident, it became clear Canada Post was not to blame.  Instead, most of the accounts were accessed because customers were using the same login credentials across multiple sites, with Canada Post being one of them.

As a result, if a user's account was hacked on another website, and the user had the same login credentials on Canada Post, then the hackers could access the Canada Post account as well.

## What should your company do to protect itself from credential stuffing?

***First,*** implement 2-Factor Authentication for account logins. This requires email or phone verification along with the standard username and password.

***Second,*** use different passwords for every account and program your employees access. If one account is hacked, the hacker will not be able to access more accounts with the same password.

***And third,*** never share passwords with other people. If you have a shared account for some reason, always give the password verbally, never through electronic communication

*Threat 5*

## Accidental Sharing

We've all seen it happen, and maybe it's happened to you:  The dreaded "Reply All" to an email when you only meant to reply to one or two people.  Suddenly, everyone in the office knows your true feelings about the manager.

Accidental sharing is a similar problem.  It occurs when information is shared or leaked accidentally, usually as a result of human error, not because of malware or a hacker.

Accidental sharing includes personal or business data, and it is shared through emails, unsecured forms, messaging or social media platforms, and a host of other ways.

Because accidental sharing is mostly based on human error, Straight Edge Technology sees it being a problem in 2020.  It is a particular threat to companies where large numbers of employees have access to primary databases.

EA Games recently had an accidental sharing incident during their FIFA 20 Global Series online competition.

When players registered for the event, they entered their sign-up information on EA Games' website.  However, the registration form contained personal information of players who had already signed up for the competition.

Obviously, the players were upset with their information being displayed.  It was especially upsetting because it didn't appear EA Games was hacked.  The issue was an accidental sharing issue inside EA Games, not the result of a cyberattack.

When EA Games became aware of the issue, they shut down the registration for several days as their IT team fixed the problem

## What should your company do to protect itself from accidental sharing?

***First,*** limit the number of employees who have access to data. The more people who have access to information, the more likely human error will cause a problem.

***And second,*** implement user activity monitoring software. This will allow you to track and discover if your data is in danger.  It also provides solutions to prevent accidental sharing.

# Conclusion

In a world where the internet connects everything, cybersecurity has never been more critical.

While having IT services and updated software and hardware  are important, it is essential to understand that today's hackers are also targeting humans through social engineering hacks.

Thankfully there is training, software, and help available for individuals and small businesses!

If you are a small business, Straight Edge Technology highly recommends you partner with an IT service provider.  Even if you have your own IT department, it is good to receive coaching and another set of eyes on your company's security.

If your business is looking for IT services in the San Antonio or Corpus Christi areas, then contact Straight Edge Technology today.  We would love to talk with you, discuss your company's goals, and plan how your IT can work for you in growing your business!

STRAIGHT EDGE
TECHNOLOGY

# 5 TOP CYBERSECURITY THREATS & SOLUTIONS

As a small business owner, you know how important your security and data are.

You also know that hackers are constantly trying to access and steal your sensitive data such as customer information, employee records, and other business data.

Straight Edge Technology has provided 5 of the top cybersecurity threats that small businesses will face in 2020.

## Keep reading to learn about these threats and their solutions!

## Phishing 1

### What is it?

Phishing is an attack that depends on social and human interaction. It occurs when a hacker uses a false identity to trick someone into providing sensitive information or data.

### Why is it a concern in 2020?

With employees using email and instant message for the majority of office communication, hackers will try to obtain employee login information and other company records by posing as a customer or coworker.

### What can be done to protect against phishing?

- First, watch for unusual emails and instant messages. They may start with unusual wording such as "Dear Customer" instead of using your name, and they often have a generic signature.
- Second, be cautious in clicking links or giving sensitive information, even if it appears to be legitimate. If in doubt, directly contact the source to make sure they sent the message.
- And third, install anti-phishing toolbars on internet browsers. These toolbars alert you to sites containing phishing information.

## 2 Malware and Ransomware

### What is it?

Malware is any malicious software attack such as worms, viruses, or Trojan horses.

Ransomware involves the hacker locking the victim's computer and files and holding the information for ransom.

### Why is it a concern in 2020?

With almost all businesses keeping their dataon servers connected to the internet, hackers are always wanting to break into this data.

With almost all businesses keeping their dataon servers connected to the internet, hackers are always wanting to break into this data.

### What can be done to protect against malware and ransomware?

- First, make sure you keep all your computer software and hardware updated. Outdated software, drivers, and other plugins are common security vulnerabilities.
- Second, enable click-to-play plugins that keep Flash or Java from running unless you click a link. This reduces the risk of running malware programs with Flash or Java.
- And third, removing old software, sometimes referred to as Legacy Apps, reduces risk.

## Database Exposure 3

### What is it?

Database exposure occurs when database informatio is exposed to hacking or theft.

### Why is it a concern in 2020?

Most companies keep their customer databases stored online. Being able to access these databases would provide hackers with sensitive customer and employee information.

### What can be done to protect against database exposure?

- First, if you have a private server, keep the physical hardware in a secure and locked room.
- Second, make sure you have a database firewall and web application firewall.
- Third, keep access to the server limited. Each person with a login to the server is a potential leak, so the fewer logins the better.
- And fourth, encrypt the data on the server and keep a regular backup.

## 4 Credential Stuffing

### What is it?

Credential stuffing occurs when someone uses the same login credentials for multiple programs and websites.

### Why is it a concern in 2020?

Because most business programs use online programs, employees are faced with a large number of logins and may use the same login credentials for multiple programs.

### What can be done to protect against malware and ransomware?

- First, implement 2-Factor Authentication for account logins. This requires email or phone verification along with the standard username and password.
- Second, use different passwords for every account and program your employees access. If one account is hacked, the hacker will not be able to access more accounts with the same password.
- And third, never share passwords with other people. If you have a shared account for some reason, always give the password verbally, never through electronic communication.

## Accidental Sharing 5

### What is it?

Accidental sharing occurs when data is accidentally shared or leaked by a company.

### Why is it a concern in 2020?

Because it is based on human error, accidental sharing will be a problem as long as humans are involved in business.

### What can be done to protect against accidental sharing?

- First, limit the number of employees who have access to data.
- And second, implement user activity monitoring software. This will allow you to track and discover if your data is in danger.