2026 EDITION

REVISED & UPDATED

Cybersecurity

Tips and Best Practices

Tier 3 Technology Solutions | www.gotier3.com

2665 SE Oak Tree Court, Ste 101, Ankeny, IA 50021 | Phone 515.512.4213 | Email: ask@tier3technology.com

Why is Cybersecurity Important?

Why is Cybersecurity such an important part of any organization?

- **A cyberattack can be devastating.**

The estimated cost of a cyberattack can range from tens of thousands to over a million dollars. It's hard to put an exact figure on the financial toll because hacking comes with many **hidden costs** — including intangibles like loss of intellectual property and devaluation of your brand.

Cyberattacks also force organizations into unwanted downtime. With your network down and your data compromised, your team members won't be able to work.

This allows the competition to surge past you, causing long-term damage to your bottom line.

Cyberattacks continue to increase in frequency, and new attack vectors emerge constantly.

Cybersecurity can feel overwhelming, but a good security profile starts with a few simple steps.

- **You need to ensure your organization is protected.**

No matter what your organization looks like, it can be a target for hackers. In fact, the federal government has warned that smaller organizations might be at a **higher risk** than large enterprises. That's because small businesses tend to be less protected and have highly valuable customer data.

This guide will explain some of the known threats out there and cover some of the steps you can take to protect your organization against bad actors.

JUMP TO...

The 4 Stages of an Effective Security Posture

A strong security posture includes **four stages**, each of which is equally important. To achieve the highest level of safety possible, you will need to invest in fortifying your organization's capabilities in each stage:

1. Prevention

Prevention is the bedrock of a good security posture. You can prevent attacks by minimizing the opportunities for cyber-attackers to enter your network in the first place.

An MSP can help you enormously at this stage by monitoring your network, implementing user controls, and educating your workforce so that everyone is alert to scams.

2. Detection

No matter how careful you are, cyber threats are inevitable. That's why it's so important to carry out thorough **threat detection**. If you can spot attacks before they reach you, you can evade those attacks.

An MSP can help make sure that you have the technology and the know-how to detect and identify an attack when it does get through your network protections. They can run a combination of detection and diagnosis and come up with the correct response to any problem that does arise.

JUMP TO...

Why is Cybersecurity Important? | 4 Stages of an Effective Security Posture | Most Common Cyberattacks | Basic Best Practices | Advanced Best Practices | Next Steps | Back to Top

3. Response

Having the correct response to threats is a game changer. After an attack is detected, you need to be prepared to quickly protect yourself from whatever is threatening your network.

A good MSP is poised to respond quickly. They can patch your software or quarantine infected devices or servers, minimizing the overall damage to your network.

Taking the right steps at the right moment, and taking those steps **decisively**, can make all the difference when it comes to your organization's resilience in the face of an attack.

4. Recovery

No matter how well you prepare, there is always the possibility you will be hit with a damaging cyberattack. If this does happen, you will need to have an effective **backup and recovery** plan in place.

An MSP can help you create and implement a solid recovery plan. That means a comprehensive data backup and recovery plan, as well as replacement servers and devices as needed.

JUMP TO...

Why is Cybersecurity Important? | 4 Stages of an Effective Security Posture | Most Common Cyberattacks | Basic Best Practices | Advanced Best Practices | Next Steps | Back to Top

The Most Common Cyberattacks

Hackers are constantly adapting and coming up with new attack vectors and strategies. There is an almost **unlimited number** of cyber threats that hamper organizations today. Threat actors are constantly on the lookout for new ways to exploit a network's vulnerabilities and stay ahead of cybersecurity measures.

That said, there are certain types of attacks that occur more frequently. While you should always be alert to new types of threats, it's a good idea to learn as much as you can about the most commonly deployed attack vectors.

Here are a few of the most common cyberattacks.

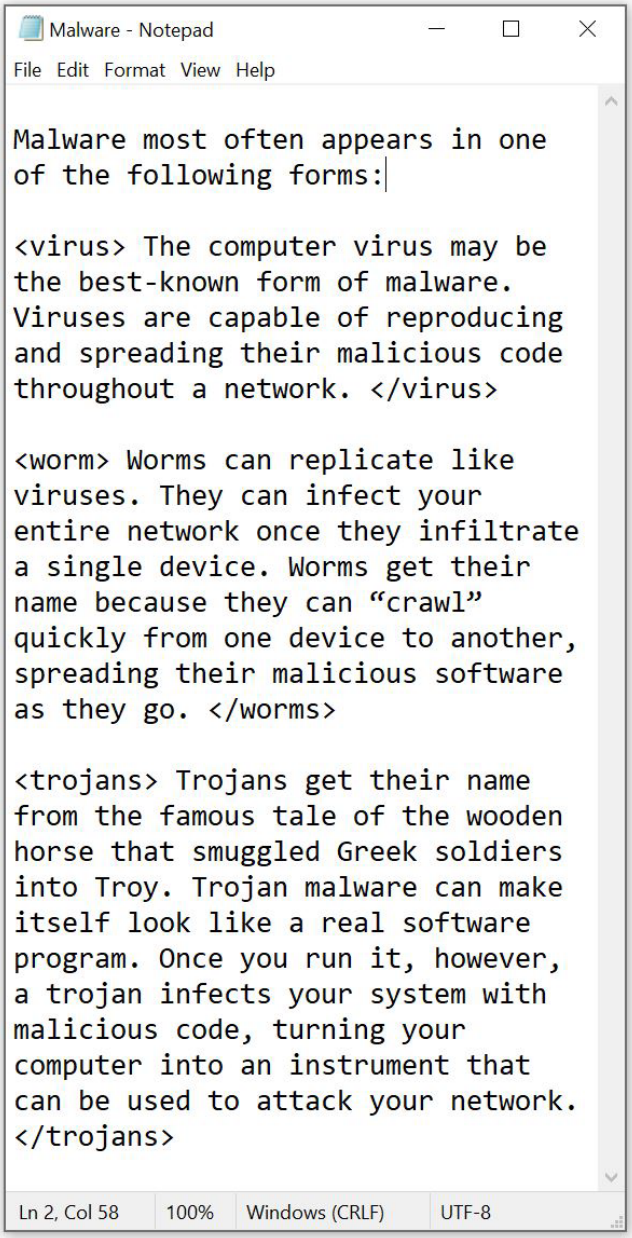
↓

The Most Common Cyberattacks

Malware

Malware is an umbrella term that refers to malicious software that is introduced into your network without your knowledge. The software is created to harm either a particular computer or a server, or to **infiltrate your network** for malicious purposes. Malware is often used to steal passwords or other personal information that makes it easier for hackers to gain access to other networks.

Malware can be difficult to detect, which makes it a tough problem for many organizations. There is a **wide range** of malware out there, making it even more difficult to spot it when it appears.



JUMP TO...

Why is Cybersecurity Important? | 4 Stages of an Effective Security Posture | Most Common Cyberattacks | Basic Best Practices | Advanced Best Practices | Next Steps | Back to Top

The Most Common Cyberattacks

▶ Spyware

As its name suggests, spyware acts like an undercover agent inside your network. Once it's introduced, it goes to work collecting your passwords for various sites. It also combs through your browsing history and any other private data that might be valuable to a threat actor.

▶ Denial of Service

A denial-of-service attack, also known as distributed denial of service, makes it virtually impossible for people to access your website.

This form of attack is commonly carried out against large organizations or agencies. However, it strikes small businesses, as well.

In a denial-of-service attack, hackers overwhelm a website or network by sending a huge stream of web traffic to it. The traffic is so intense that it forces the website or server to shut down so that customers cannot access it.

Denial-of-service attacks are **increasingly common**, and they don't always seem to follow logic or reason.

If you ever suspect that you may be the target of a denial-of-service attack, it's a good idea to limit traffic on your site and set up software that can monitor the traffic flow at different times of the day.

JUMP TO...

Why is Cybersecurity Important? | 4 Stages of an Effective Security Posture | Most Common Cyberattacks | Basic Best Practices | Advanced Best Practices | Next Steps | Back to Top

The Most Common Cyberattacks

Man in the Middle

A man-in-the-middle attack allows hackers to read emails or text messages between you and others in your network. This means that cyber-attackers can read your communications with your business partners and staff. Although there are many subtle variations, part of the allure of this attack for many threat actors is its simplicity: a basic man-in-the-middle attack is **one of the easiest attack vectors to learn**.

Most people have heard warnings against trusting open Wi-Fi networks, but they don't know why. Precisely because many of these users continue to use open Wi-Fi networks, there is a tremendous opportunity and incentive for threat actors to employ this attack method. Avoiding open wireless networks is a simple way to deny would-be attackers an open invitation to your data, but it's only one method of prevention.

> **Avoiding** open Wi-Fi networks is a simple way to help protect your data.

A man-in-the-middle attack is the perfect mechanism for hackers to steal secrets and privileged information. There are indications that this type of attack could be on the rise, especially with more employees working remotely. Remote workers often use unsecured networks to send and receive information, making them susceptible to man-in-the-middle attacks. If part of your workforce is remote, it would be a good idea to deploy **end-to-end encryption** on your network-facing devices so you don't fall victim to this kind of attack.

JUMP TO...

Why is Cybersecurity Important? | 4 Stages of an Effective Security Posture | Most Common Cyberattacks | Basic Best Practices | Advanced Best Practices | Next Steps | Back to Top

The Most Common Cyberattacks

In recent years, man-in-the-middle variations have grown more complex. Cyber-criminals are devoting energy and resources to countering the rise of preventative measures like multifactor authentication (MFA) and security training. **MFA-bypass kits**, for example, are becoming more popular. One such kit is the triple reverse proxy, which can insert an attacker into an existing browser session. This is much more effective than luring the user to a facsimile, which can contain recognizable flaws that team members may be trained to spot. By presenting the end user with the actual site, threat actors can more effectively camouflage themselves and harvest cookies, which allows them to access your account without your password or username.

▶ Personal-Device Attack

Personal- and mobile-device attacks are becoming more common. The rise of the "bring your own device" workplace means that more employees are using their personal phones and tablets for work. Unfortunately, employees are not always careful about securing these devices, making them an easy target.

It's a good idea to implement an organization-wide mobility management program to protect all your endpoint devices. It's also a good practice to have your employees use **multifactor authentication** on their phones or tablets. Organizations can further protect themselves by making this a condition of allowing employees to work on their own devices.

JUMP TO...

Why is Cybersecurity Important? | 4 Stages of an Effective Security Posture | Most Common Cyberattacks | Basic Best Practices | Advanced Best Practices | Next Steps | Back to Top

The Most Common Cyberattacks

Ransomware

Ransomware takes your computing network hostage. It typically works by encrypting specific files that you need to do your work and refusing to grant you access until you pay a ransom to the hackers who launched the ransomware.

It's important to note that ransomware, like all attack vectors, continues to evolve.

As more organizations have recognized the pivotal role that comprehensive data backup and disaster planning plays in undermining the efficacy of ransomware attacks, bad actors have responded by escalating the complexity of their attacks. A **stacked ransomware attack**, for example, incorporates multiple attack vectors and can even involve collaboration with other threat actors who specialize in specific tactics including targeting backups.

> **Ransomware** paralyzes your data and takes your network hostage.

In a "stacked" configuration, a ransomware attack becomes much more effective. A threat actor can encrypt your data, paralyze your operations, and then exfiltrate and access this data. In what is known as a "double extortion," an attacker can put additional pressure on your organization by threatening to publish your sensitive information online. But recently, a **triple extortion** method has emerged, which has increased the pressure that threat actors can put on organizations. Leveraging their access to your sensitive data, an attacker doesn't need to stop at merely threatening your organization. They can now threaten your clients and/or suppliers— anyone whose sensitive information

JUMP TO...

Why is Cybersecurity Important? | 4 Stages of an Effective Security Posture | Most Common Cyberattacks | Basic Best Practices | Advanced Best Practices | Next Steps | Back to Top

you've been storing. In a triple extortion, attackers threaten your reputation by targeting those who placed their trust in you. Triple extortions can also involve the threat of leaking data to the media—publicizing not only your data but also the sensitive information of those who trusted you to keep their records secure.

▶ Phishing

Finally, we come to phishing.

Phishing attacks often use malware, but it's the method by which this malware is delivered that makes a phishing attack a **unique and unpredictable** threat.

A phishing attack disguises itself as a real message, but it's actually a sneaky way to get malware onto your device. Typically, phishing attacks come in the form of emails or text messages. They're often disguised to look like they're coming from a person or business you know.

Be on your guard against phishing attacks. Never give out your password or other private information in response to an email or text message. No legitimate organization will ask you to do so.

> **Phishing** attacks have become much more sophisticated.

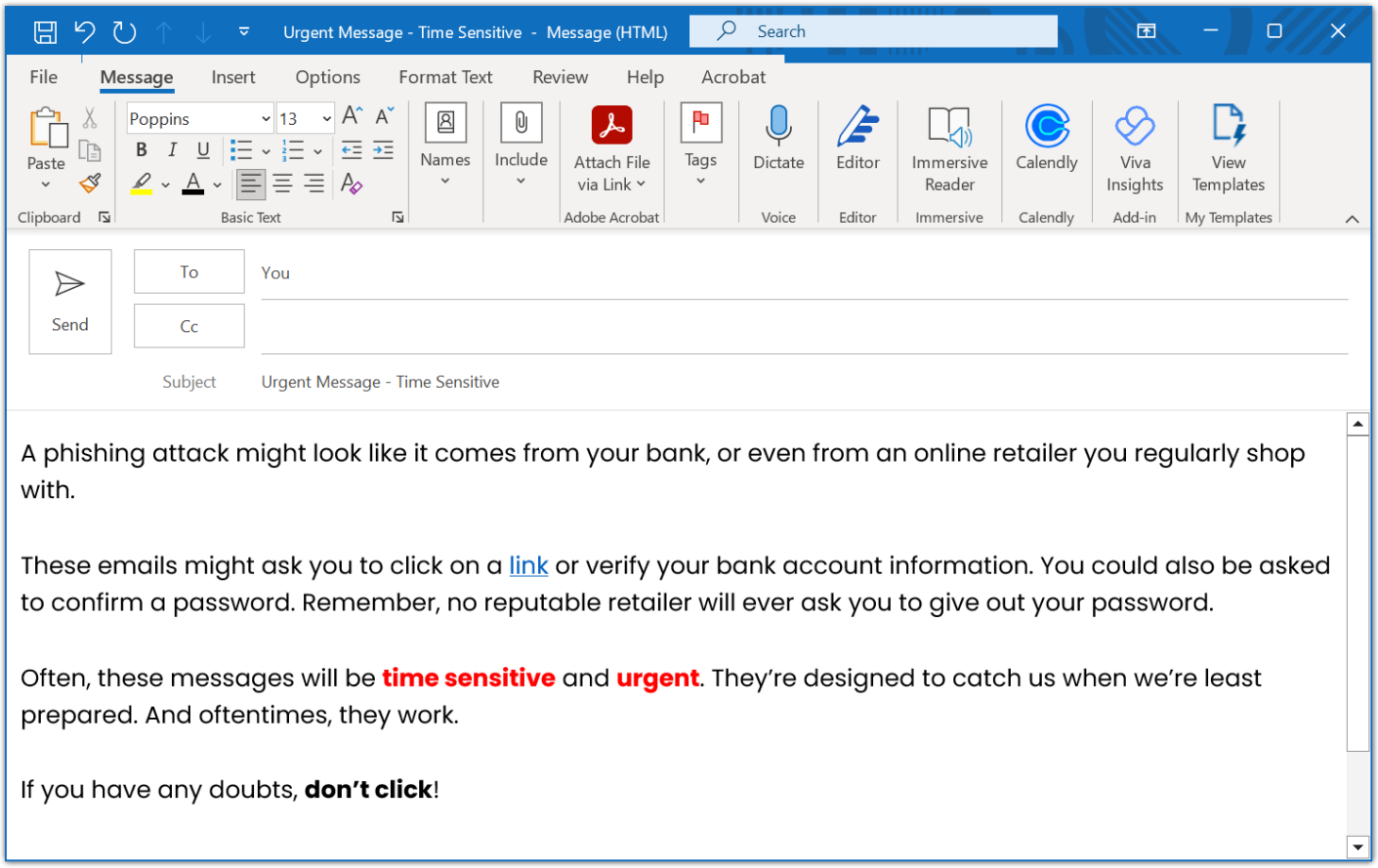
You should also **never click** on a link if anything about the email looks suspicious in any way.

JUMP TO...

Why is Cybersecurity Important? | 4 Stages of an Effective Security Posture | Most Common Cyberattacks | Basic Best Practices | Advanced Best Practices | Next Steps | Back to Top

The Most Common Cyberattacks

Phishing attacks have become more sophisticated and difficult to recognize. As more organizations have taken precautions against phishing, threat actors have evolved and implemented more advanced measures—including increasingly realistic imitations of brand aesthetic and voice.



To continue to protect themselves, organizations must invest in regular, comprehensive **awareness training** for all staff, and consistently test the efficacy of this training by sending phishing tests to staff members on a regular basis.

JUMP TO...

Why is Cybersecurity Important? | 4 Stages of an Effective Security Posture | Most Common Cyberattacks | Basic Best Practices | Advanced Best Practices | Next Steps | Back to Top

Basic Best Practices

Sometimes, small changes can make a world of difference. That's often the case when it comes to cybersecurity. Here are some relatively **simple best practices** that can improve the safety and security of your entire organization.

► Create strong, unique passwords

Ideally, a password should be at least eight characters long. It should include both uppercase and lowercase letters, at least one number, and at least one symbol. Passwords should never be birthdays, sports teams, or other easy-to-guess words and numbers. Passwords should **never be shared** with anyone, under any circumstances.

Each account should have a strong, unique password. Because threat actors have easy access to sophisticated tools, they only need to breach one password to run programs designed to probe millions of sites for matching user/password entries.

In fact, it's wise to proceed with the assumption that each password you create will eventually be compromised, and to prepare accordingly. By creating a unique password, you limit your exposure to that account, which is a great first step. Multifactor authentication on **every account** is a great additional security measure—at the very least, all of your most sensitive accounts should be protected by multifactor authentication measures.

JUMP TO...

Why is Cybersecurity Important? | 4 Stages of an Effective Security Posture | Most Common Cyberattacks | Basic Best Practices | Advanced Best Practices | Next Steps | Back to Top

Basic Best Practices

▶ Keep your software up to date

Software firms are continually monitoring for new forms of cyberattacks. When they update their software, it's because they want to patch up the vulnerabilities in their original product.

Make sure that you update your software regularly so that you get the latest protection against cyberattacks. However, it's important that organizations never assume automatic updates are working without human oversight. There are many variables that routinely disrupt and delay automated updates. The process is often disrupted by machines being offline during update windows and by staff members delaying or ignoring update prompts. Even if an organization is strong in every other security area, a lack of careful oversight when it comes to updates an very quickly undermine those efforts and compromise an entire IT environment.

▶ Secure your personal devices

This goes for your entire staff. If you're working on a mobile phone, tablet, or laptop, make sure that you have all the latest security measures installed. After all, if your device becomes infected, an attack could spread to the **entire network**.

JUMP TO...

Why is Cybersecurity Important? | 4 Stages of an Effective Security Posture | Most Common Cyberattacks | Basic Best Practices | Advanced Best Practices | Next Steps | Back to Top

Basic Best Practices

▶ Don't click on questionable links

If you see something suspicious, don't click on it. Hackers love to use links to infect your device and infiltrate your network. Be on the lookout for **suspicious links**. If words are misspelled, or the website logo doesn't look quite the same as usual, there is probably something wrong. Don't click.

Dear colleagues,

We are pleased to present to you our mobile enterprise application. The app offers company-related news, access to HR data, events, and a messaging interface for internal communication. It will soon be available for download for IOS and Android.

Before the public release, we ask our employees to download the application as a desktop version and report any problems that occur.

We are looking forward to your feedback!

Thank you!

↑

(Questionable link in action)

When in doubt, don't click.

Basic cybersecurity practices are a good start. On their own, though, they won't offer maximum protection to your organization. Next, we'll cover some advanced best practices.

JUMP TO...

Why is Cybersecurity Important? | 4 Stages of an Effective Security Posture | Most Common Cyberattacks | Basic Best Practices | Advanced Best Practices | Next Steps | Back to Top

Advanced Best Practices

Next-generation antivirus

Antivirus software isn't enough to protect your entire network. While it's a good basic practice, the best practice is to invest in next-generation antivirus software. Traditional antivirus software isn't enough. Ransomware, for example, works too fast for traditional antivirus software. Next-generation antivirus software, however, can look for and identify **dynamic patterns and behaviors** that traditional antivirus isn't equipped to recognize. But, like all components of an organization's security infrastructure, even next-generation antivirus software needs consistent oversight to operate at maximum effectiveness.

Proactive cybersecurity

A proactive security approach means that you look out for problems before they arise, and you take steps to protect yourself ahead of time. A proactive approach puts you in a position of **power and security**.

On the other hand, a reactive security approach means that you don't take any action until after a problem has revealed itself. A reactive approach may mean that you scramble to pick up the pieces after a ransomware attack, or after hackers have crashed your network.

JUMP TO...

Why is Cybersecurity Important? | 4 Stages of an Effective Security Posture | Most Common Cyberattacks | Basic Best Practices | Advanced Best Practices | Next Steps | Back to Top

Advanced Best Practices

Next-Level Services

A quality managed service provider (or MSP) can proactively introduce services to help **keep your organization secure** from cyberattacks. Those services may include network security scanning, 24-hour network threat monitoring, and employee education.

As you'll see, partnering with an MSP can help you establish a highly effective security posture.

JUMP TO...

Why is Cybersecurity Important? | 4 Stages of an Effective Security Posture | Most Common Cyberattacks | Basic Best Practices | Advanced Best Practices | Next Steps | Back to Top

Next Steps

Hopefully, this piece has given you a sense of what some of the biggest cyber threats look like and how you can mitigate them. However, there's still a missing piece of the puzzle. **Every organization is unique**.

Which threats are particularly dangerous for your organization? What are your vulnerabilities? What does your organization's unique security posture look like today?

Each organization has slightly different security needs. That's why it's always a good idea to consult with a managed service provider to discuss the best approach to protecting your organization.

> Every organization has **unique** security needs.

A qualified MSP like **Tier 3 Technology** can carry out a top-to-bottom assessment of your network and identify all your existing vulnerabilities. We can assess your level of risk and highlight areas of improvement.

Improving your security posture may sound like a daunting task. But it's just a matter of working steadily toward a goal. When you team with Tier 3 Technology, we'll help you with every stage of the process, including reviewing your internal processes and investing in employee education.

This **strategic partnership** can help you create stronger endpoint protections that help shield your data at every point.

JUMP TO...

Why is Cybersecurity Important? | 4 Stages of an Effective Security Posture | Most Common Cyberattacks | Basic Best Practices | Advanced Best Practices | Next Steps | Back to Top

Next Steps

Want to learn more? Visit our website.

Our Story: https://youtu.be/XFKHGZPmvhU.

Want a quote now? Take the fast track and get the conversation started!

TIER 3 TECHNOLOGY

JUMP TO...

Why is Cybersecurity Important? | 4 Stages of an Effective Security Posture | Most Common Cyberattacks | Basic Best Practices | Advanced Best Practices | Next Steps | Back to Top