GCA Cybersecurity Toolkit for Small Business Handbook

Welcome

Dear Colleague:

The Internet is an integral part of most companies' business these days. Securing your business's digital ecosystem must be part of how you work. A cyberattack can have devastating consequences including financial loss, theft of sensitive information, compromised supply chains, and more.

You have many other concerns and responsibilities, and we have worked to provide a resource that you can actually use to address your cybersecurity needs. The Global Cyber Alliance (GCA) Cybersecurity Toolkit for Small Business provides free and effective tools to reduce your cyber risk. The tools are carefully selected and organized to make it easy to find and implement important steps that will help defend your business against cyber threats. We've included videos as well as a community forum where you can find support and get questions answered from your peers and security experts. The toolkit is designed for you, not a hypothetical small business with cybersecurity experts on staff and a large budget.

The GCA Cybersecurity Toolkit for Small Business Handbook is a companion to the toolkit to help guide you through its use. You can download the handbook in full, or chapter by chapter, as you work your way through the recommended actions in the toolkit. This guide facilitates your ability to work at your own pace to take action and will be a handy reference document at your convenience.

These resources will be regularly updated with input from users, industry experts, and partners across the globe.

We hope you will take advantage of the toolkit and handbook to start improving your cybersecurity today!

Sincerely,

Philip Reitinger
President and CEO

Table of Contents

Handbook Chapters

Know What You Have

What Problem Does This Toolbox Address?

Knowing what you have is the first step to better security simply because you cannot protect what you do not know you have. Consider that many cyberattacks and data breaches are caused by lost or stolen laptops and other devices, unauthorized access to accounts, and unpatched software vulnerabilities. By knowing what computers, devices, and software you have (i.e., your assets), you will better understand potential risks that might exist, which will enable you to make informed decisions and take steps to reduce those risks.

- Do you know how many laptops and mobile devices your business has, who has access to them, and what software and applications are on them?
- Do you know how old your computers are and when you last updated their security?
- Do you have any systems or devices connected to the Internet (such as security cameras or building controls) that are also connected to your business network?

These assets could offer a route into your business environment that a hacker could use to steal or corrupt your data. Clearly, knowing what devices and systems you have is important. Some of your assets are more critical for business operations than others, and having a complete, up-to-date inventory helps you prioritize what needs to be protected and at what level.

What Will This Toolbox Help You Accomplish?

After completing this toolbox, you will better understand:

- ✔ **how to conduct an inventory of your data and systems**
- ✔ **which devices and applications are critical for your business operations**

How To Use The Toolbox

Use the tools in the **Know What You Have Toolbox** to help you identify all of your devices (including desktops, laptops, smartphones, and printers) and applications (e.g., email, software, web browsers, and websites) so you can take steps to secure them.

This inventory will serve as a guide and checklist as you make your way through the rest of the toolboxes. Ensure you keep your inventory up to date, including whenever you add or delete new equipment, accounts, or critical data.

Download the tools from the website and note the dates completed. Also, take this opportunity to schedule a regular review to ensure all your information is up to date.

Navigating the Toolbox Subcategories and Additional Information to Consider

1.1 Identify Your Devices

When creating an inventory it is important to consider everything in your environment.

This includes items such as desktops, laptops, smartphones, printers, CCTV, PoS, IoT devices, and routers.
Many consumer IoT devices have no, or very minimal, built-in security so consider whether it may be possible to separate them from the rest of your network or remove them completely.

Older equipment may be out of warranty and no longer protected against new vulnerabilities but are important to business operations. These should be identified as part of your inventory and a plan developed to either replace, upgrade, or restrict their use.

Many devices such as routers, CCTV, and printers are sometimes forgotten when thinking about the IT environment, but anything that has a connection to the Internet or the local network should be considered when you are doing your asset inventory because these connections will often provide a potentially easy route into your business.

Identify where sensitive and business critical data is held - whether that be on standalone, network-connected devices or in the cloud. It may be that additional levels of protection should be considered for these devices, but step one is to document where everything is kept.

1.2 Identify Your Applications

Identify all of your applications including business applications, online accounts for which you use your business email address, and other applications you access either locally or remotely via your devices.

It is important to consider all applications and accounts, remembering ones you no longer use in particular as you are unlikely to be updating software for these. If they provide no benefit to you then remove them or close the accounts. An old online account may hold some of your personal information, and if the organization you originally set that account up for gets breached your data could be affected.

Additional information, support, and guidance during implementation is available via the **Know What You Have Category** on the GCA Community Forum.

Know What You Have Links:

Toolkit:

Know What You Have Toolbox
https://gcatoolkit.org/smallbusiness/know-what-you-have/

Community Forum:

Know What You Have Category

https://community.globalcyberalliance.org/c/cybersecurity-toolbox/know-what-you-have/

Update Your Defenses

What Problem Does this Toolbox Address?

Cybercriminals look for weaknesses and flaws (known as vulnerabilities) that can be used to gain access to systems or spread malicious software. Malicious actors could gain access to your company's financial accounts, your customers' data, and much more. You can help protect against this by updating your defenses (i.e., keeping your systems, devices, and data updated). Manufacturers and software developers regularly release security updates for their operating systems and applications to address newly discovered weaknesses or vulnerabilities. These fixes are usually referred to as patches, and the process is known as patching.

This toolbox addresses the need to apply these patches in a timely manner, including setting up (also called configuring) systems so they can be applied automatically whenever possible. Additionally, it is important to realize that over time many systems are added to, adapted, or reconfigured which may lead to the introduction of weaknesses that could be exploited by cybercriminals. Another issue to keep in mind is whether a third-party supplier has access to data within your systems. Keeping up-to-date records is important; it allows you to manage the updates necessary to ensure the most current patches are applied to your systems, devices, and applications.

What Will This Toolbox Help You Accomplish?

After completing this toolbox, you will better understand how to:

- ✔ check that you are running the latest version of software on your device
- ✔ set your devices to automatically accept and apply security updates
- ✔ implement secure configuration settings for mobile devices, web browsers, and operating systems

How To Use The Toolbox

Use the tools in the **Update Your Defenses Toolbox** to ensure your devices and applications are set with the latest security patches applied and with the appropriate levels of security for the type of data they contain. If you created an inventory in the Know What You Have Toolbox, use this as a guide and checklist to ensure all your devices are updated and are set to automatically accept security updates.

Once you have completed the Update Your Defenses Toolbox, update your Security Checklist and set a reminder to repeat this process periodically so it becomes routine.

Navigating the Toolbox Subcategories and Additional Information to Consider

2.1 Update Your Devices and Applications

When a solution, or patch, is developed and released for a known vulnerability, it is important that all users of that system or application apply these patches immediately - ideally automatically because until that is done they are at risk of compromise via this vulnerability.

Check each device and application, and configure them to automatically update. We have provided a list of the most common systems and applications, but for those not covered in this toolbox check the instructions or support pages for that particular device or application. Check each item off your list as you go, and be sure to take this step every time you add a new device or application to your business.

Often the most secure settings are not provided as the default out-of-the-box security setting (known as configuration) for your devices or applications, because ease of use and convenience are prioritized over security. Therefore, you should check if there are any manufacturer recommended security configurations for your devices and applications and implement those.

Any devices that are no longer supported should be removed, because they will always be at risk of compromise from any newly discovered weakness. If this is not possible then they should be isolated from other devices and their use restricted to specific business functions only.

The tools found in this toolbox offer configuration guidance for common systems to automatically apply updates. You should check the guidance for all your devices and systems to make sure they are set accordingly.

2.2 Encrypt Your Data

If your computer network does suffer a breach there is a high probability that the hacker will be looking to steal sensitive or confidential information, which they may use for their own financial or political gain. By encrypting data that is stored on your hard drive it makes it much harder for criminals to make use of this data because it will need to be decrypted before it is usable.

Encryption is the process whereby data is converted from a readable form (i.e., plaintext), to an encoded form (i.e., ciphertext). This encoding is designed to be unintelligible except by parties that possess the “key(s)” to reverse the encoding process. Encryption allows for the confidential storage and transmission of data as well as proof that it originated with the person who claims to have sent it.

These tools allow you to encrypt files stored on your hard drive. If your operating system is not included in the toolbox here, further options may be available via the equipment manufacturer or other commercially available security offerings.

2.3 Secure Your Websites

For many businesses your website is critical to business operations. Its use may include the flow of sensitive information across the supply chain or it may be the main trading platform on which your

business relies. Should hackers gain access to the website they could intercept or steal data, change its contents, infect the website with malware, or take over operations. Any of these could have a devastating impact on your organization's ability to operate.

Here you will find tools you can use to run regular checks on your website (known as scans) to identify vulnerabilities and potential weaknesses. Ensure any identified problems are assessed by IT-competent personnel and the appropriate action taken.

The toolbox subcategories provide instructions and tools for commonly used systems. For others, search for help via the vendor website or ask for advice in the GCA Community Forum **Update Your Defenses Category** or **Small Business Community**.

Update Your Defenses Links:

Toolkit:

Update Your Defenses Toolbox
https://gcatoolkit.org/smallbusiness/update-your-defenses/

Community Forum:

Update Your Defenses Category
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/update-your-defences

Small Business Community
https://community.globalcyberalliance.org/c/community-discussions/small-business-community/

Beyond Simple Passwords

What Problem Does This Toolbox Address?

Passwords are a first line of defense in protecting your accounts and data (such as email, personnel records, or client databases).

Unfortunately, passwords are often an easy target for cybercriminals, and hacking-related data breaches often occur because of weak passwords. Attackers have many ways to try and access your passwords, from using easily obtainable password crackers, which are programs that cycle through commonly used combinations to using a username and password obtained from an account that

suffered a breach - trying those on other popular sites. These techniques need little technical ability, are fast, fully automated, and are readily available to those who know where on the Internet to look for them. Compounding the problem for small and medium-sized businesses is that many do not have a password policy, or if they do, they do not strictly enforce it.

So having strong passwords is vital to protect your data. But you also need to take it another step further by implementing two-factor or multi-factor authentication (2FA).

2FA requires multiple credentials, making it much harder for an attacker to gain access to your accounts. With 2FA, a user needs the following:

- Something you know, such as a password;
- And something you have, such as a token (Google Authenticator, Authy, Okta, RSA, etc.) or a verification code sent to your phone; or
- Something you are, such as your fingerprint or face (biometrics).

This toolbox helps you create stronger, unique passwords for each of your accounts and shows you how to set up 2FA, both of which are important steps in protecting access to your accounts and data.

What Will This Toolbox Help You Accomplish?

After completing this toolbox, you will better understand how to:

- ✔ create a strong password
- ✔ test your accounts to see if they have been compromised
- ✔ set up 2FA for most common online accounts

How To Use The Toolbox

Use the tools in the **Beyond Simple Passwords Toolbox** to ensure your devices and applications are set up with strong passwords and 2FA. If you created an inventory in Know What You Have, use this as a guide and checklist to ensure you have implemented it across all your accounts.

Once you have completed the Beyond Simple Passwords Toolbox update your Security Checklist, and set a reminder to repeat this process periodically so it becomes routine.

Navigating the Toolbox Subcategories and Additional Information to Consider

3.1 Strong Passwords

One of the most common methods criminals use to gain access to your accounts, network, and information is to log in as you. It is really important that you:

- Use a unique, strong password (or passphrase) for each of your accounts.
- Use letters, numbers, and special characters to ensure a strong password.
- Change your password immediately if you have been breached.
- Keep your passwords private and safe.
- Never reuse a password.
- Never click on a link in an email telling you “it is time to reset your password;” always access the account website via the web browser.
- Avoid signing into accounts via public Wi-Fi.

Using the same password across multiple accounts means that if a criminal gets one of your passwords, they have effectively gained access to all of your accounts that use it. Username and password details may be sold online by criminals who have stolen them in a cyberattack and be reused until the password is changed. Rapid technology advancement means that a cheap modern laptop can quickly cycle through all combinations to work out short simple passwords.

You should have a password policy that is understood and adhered to by all staff and any contractors who have access to your systems. Some systems and applications may enable you to enforce a minimum allowable password so this is certainly worth checking in the security settings.

You can use the tools in Strong Passwords to learn more about passwords and to check whether your email address has been stolen in a breach. If it has, then change your password immediately and never reuse passwords.

Remember also to check password settings on routers, printers, and other equipment connected to your network. These can easily be forgotten and are generally shipped with simple default passwords. Work through the inventory you created in Know What You Have and tick them off as you go!

3.2 Tools for 2FA

Two-factor authentication (2FA) provides an important second line of defense beyond passwords to protect accounts from unauthorized access. There are a number of different authentication methods that may be used for 2FA. These range from a unique code sent via text to your mobile phone, a hardware token you carry around, a fingerprint, or facial recognition.

Tools for 2FA contains downloadable resources that provide accepted authentication methods for many common accounts.

While implementing the tools and guidance in the Beyond Simple Passwords Toolbox, also consider what permissions each user has when accessing business-related applications. Consider restricting access only to those who need it and to the extent that their role requires.

3.3 Manage Your Passwords

Password managers are a way of keeping all your passwords together securely without needing to remember each one individually. This means that you only need to remember one password each time you want to sign into one of the accounts whose password is stored in the password manager.

Password managers do offer more convenience. However, it does also mean that if the password manager is compromised the attacker would have access to all the passwords.

Additional information, support, and guidance during implementation is available via the **Beyond Simple Passwords Category** on the GCA Community Forum.

Beyond Simple Passwords Links:

Toolkit:

Beyond Simple Passwords Toolbox
https://gcatoolkit.org/smallbusiness/beyond-simple-passwords/

Community Forum:

Beyond Simple Passwords Category
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/beyond-simple-passwords/

Prevent Phishing and Malware

What Problem Does This Toolbox Address?

Every year many small businesses fall victim to costly malware and phishing attacks. When a user clicks on a website infected with malware or opens an infected attachment in a phishing email, the result can be deleted or altered files, modified applications, or disabled system functions.

Malware is any software that is designed to cause damage to and/or unauthorized access to devices or networks. Phishing emails trick the user into believing they are dealing with a trustworthy entity so the attacker can gain unauthorized access to private, sensitive, restricted content, or money. The attacker will do whatever they can to make their email appear genuine and enticing to get the user to click or open. The emails may look like they come from someone you know, they might mimic the logos and format of emails from well-known organizations, or they might refer to recent headlines or a job you have just done.

Some estimates suggest that more than 90% of cyberattacks start with a phishing email. If you click on the link or open the attachment in a phishing email, you might trigger any number of activities that the attacker has set up which could include stealing your data, creating a secret route (known as a backdoor) into your computer for later use, installing a type of malware through which the attacker locks you out of your data and demands you pay a ransom for access (known as ransomware), or downloading another type of malware that allows the attacker to see what you type in, such as passwords or account numbers (known as spyware).

The consequences of phishing and malware attacks are severe for small businesses. The effects can include loss of or damage to data, loss of income if your business is shut down during an attack, expenses incurred to repair/replace equipment, costs to notify customers or clients of a breach, along with loss of reputation and potential lawsuits.

What Will This Toolbox Help You Accomplish?

The **Prevent Phishing and Malware Toolbox** will help you reduce risks by strengthening your resilience to attacks. Included are tools to help prevent you from going to infected websites, anti-virus software to help prevent viruses and other malware from getting into your systems, and ad blockers to help prevent online advertisements which can carry viruses.

After completing this toolbox, you will better understand:

- ✔ how anti-virus software protects your systems and data
- ✔ how to install anti-virus software on your system
- ✔ digital advertisements and the risks they pose
- ✔ how to install an ad blocker to block pop-ups ads, videos, and other unwanted content
- ✔ what DNS stands for and why it is important
- ✔ how DNS security works and what types of attacks it mitigates
- ✔ how to install Quad9 on your Android devices and computers

Navigating the Toolbox Subcategories and Additional Information to Consider

The tools were carefully chosen based on recognized global standards, and they are not presented here in any particular order or recommended priority.

4.1 Anti-virus

It is important to use real-time anti-virus because this checks for viruses in real time, as they are happening thus removing viruses before they can cause damage, and it gets updated as new virus protection is developed.

4.2 Ad Blockers

Some online advertisements or messages that appear while browsing a website are useful; however, others may contain malicious code and could infect your computer with malware if you click on the ad. An ad blocker may be used to prevent advertisements appearing on web pages, offering additional protection while browsing.

4.3 DNS Security

DNS security uses the Domain Name System (which is the Internet equivalent of a phone book) to translate the text-based website name (domain name) a user types in the browser into a unique set of numbers (IP address), which computers understand.

Many attackers will try to use look-alike website domain names to trick victims into thinking they are connecting to a legitimate site. These sites may look like the real website name, but closer inspection may show differences.

So, for example, a company's legitimate website URL might look like this: "www. mygreatwidgets. com," but the fake one might look like this: "www. rnygreatwidgets. com."

DNS firewalls, which is one type of DNS security, can help prevent viruses and phishing attacks because it checks whether the IP address of the website being requested is known to harbor malicious code, and if so it will block access to it. Users can implement DNS filtering services on their systems using the tools within this subcategory to help prevent access to known malicious websites.

The toolbox subcategories provide tools for commonly used systems. For further support search or ask questions in the GCA Community Forum **Prevent Phishing and Malware Category** or **Small Business Community**.

Prevent Phishing and Malware Links:

Toolkit:

Prevent Phishing and Malware Toolbox
https://gcatoolkit.org/smallbusiness/prevent-phishing-and-malware/

Community Forum:

Prevent Phishing and Malware Category
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/prevent-phishing-and-viruses/

Small Business Community
https://community.globalcyberalliance.org/c/community-discussions/small-business-community/

Backup and Recover

What Problem Does This Toolbox Address?

The loss or corruption of data could be due to a cyberattack (such as ransomware) or by equipment failure or theft, human error, accidental damage, fire, or flood. Regardless of the cause, the impact of data loss or equipment downtime can seriously impact your business's productivity and profitability.

A backup is a copy of your data, stored in a different location than the original data, and it can help you recover from an attack or data loss. Having regular on and offline backups will facilitate a faster recovery from data loss or data corruption. Both are important because online backups are set to automatically backup across a network, whereas offline backups require the plugging in and then removal of an external device (e.g., a USB or hard drive) for physical storage elsewhere (which also helps guard against the inadvertent backing up of already corrupted data).

What Will This Toolbox Help You Accomplish?

After completing this toolbox, you will better understand:

- ✔ why backups are important for your business, especially in recovering from a ransomware attack
- ✔ how to enable full backup on your Windows or Mac machine

How To Use The Toolbox

Use the tools in the **Backup and Recover Toolbox** to ensure your systems are regularly backed up, at a level and frequency appropriate for the type of data held within.

What should you back up? That depends on your information and the risk to the loss of that information. If you created an inventory in the Know What You Have toolbox, use that as a guide and checklist updating it as you go.

Once you have completed the Backup and Recover Toolbox update your Security Checklist and set a reminder to review periodically to ensure your policy remains appropriate for your business.

Navigating the Toolbox Subcategories and Additional Information to Consider

Ransomware is one attack method that has become a serious problem for small businesses. Ransomware is a type of malicious software that infects computers and blocks access to data. The perpetrator demands payment, sometimes in the form of cryptocurrency, (i.e., bitcoin which is less easy to trace than traditional transfers) on the promise that the data will be restored once the ransom is received. Having backups for your data is an important safeguard for accessing your information if you are the victim of ransomware.

5.1 Backup Operating Systems

Having a solid backup policy which includes both on and offline backups helps facilitate a faster recovery from data loss or data corruption.

- The different data sets you hold should be categorized within the inventory (refer to the Know What you Have Toolbox for help creating an inventory).
- Consider the use of encryption for sensitive information (refer to the Update Your Defenses Toolbox for more information on encryption).
- Implement a sensible approach to backing up each data set having considered the "loss impact" for each. The loss impact may be reputational, financial, or legal.

In the Backup Operating Systems subcategory, you will find instructions for backups on common operating systems. If yours is not included, search for help via your provider website or ask in the **Backup and Recover Category** on the GCA Community Forum.

Also ensure you have a disaster recovery plan, which helps enable recovery of critical systems following a disaster (whether accidental or natural disaster). Having a plan helps minimize recovery time and damage to systems, protects against potential liabilities, and can also improve security. There are many templates and guides for developing a plan available online. Make sure you keep it updated, and conduct mock scenarios to exercise the plan and ensure everyone knows how to implement it.

Backup and Recover Links:

Toolkit:

Backup and Recover Toolbox
https://gcatoolkit.org/smallbusiness/backup-and-recover/

Community Forum:

Backup and Recover Category
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/back-up-and-recover/

Protect Your Email

and Reputation

What Problem Does This Toolbox Address?

Email is often used as the starting point for a cyberattack. It is extremely quick and inexpensive to send thousands of emails to unsuspecting recipients in the hope that at least some users will be tricked into clicking on the malicious website link or downloading the harmful attachment.

One of the techniques cybercriminals use is to make the email appear as if it has been sent from a legitimate source, such as your financial institution, a client, a business partner, or other familiar organization. One of these techniques is known as email domain spoofing, in which the "spoofed" email address used is exactly the same as the genuine one, thus making it appear to have actually been sent from that organization, giving the receiver little reason to suspect it has not actually been sent from them.

If your company email domain (the part of your email address after the "@") is spoofed this could have serious consequences for you, your customers, and supply chain. If that email recipient took action on the email because they genuinely believed it came from you this could lead to their computer system being infected with some form of malware or ransomware. It could also allow the criminal to take control and manipulate your banking details, so customers make payments into other accounts thinking they are paying you.

The Protect Your Email and Reputation Toolbox provides guidance and tools to protect against this type of threat, including guiding you through use of an email standard known as DMARC (Domain-based Authentication, Reporting, and Conformance). DMARC is an effective way to stop spammers and phishers from using company domains to carry out dangerous cyberattacks. It is a way to verify the sender of an email has permission to use your email domain and send email.

Attackers may also set up "look-alike" websites. For example, the genuine domain "BestBusiness .com" may be impersonated by registering "BestBusness .com" or "BestBusiness .net" to trick customers or users into visiting them.

If your email or website domains are spoofed it could result in damage to your reputation and brand, as well as harm to your customers. Using the tools in Protect Your Email and Reputation helps to identify and prevent impersonation.

What Will This Toolbox Help You Accomplish?

After completing this toolbox, you will better understand:

- ✔ what DMARC stands for, why it is important, and what attacks it mitigates
- ✔ the DMARC Setup Guide
- ✔ how to check your own email domain to see if DMARC is enabled

How To Use The Toolbox

Use the tools in the **Protect Your Email and Reputation Toolbox** to ensure your company is protected from email domain spoofing through the implementation of DMARC and identify potential lookalike website domains.
Update your Security Checklist once complete and encourage your customers and supply chain who use their own domain to do likewise, because DMARC effectiveness is dependent on both the sender and receiver having implemented DMARC.

Navigating the Toolbox Subcategories and Additional Information to Consider

6.1 Implement DMARC

Use the tools in this subcategory to find out more about DMARC, check whether your email domain is protected by DMARC, and if so to what level.

6.2 Understand DMARC Reports

Once a DMARC policy is set up on your email domain you will start to receive reports showing how your email domain is being used. These can be difficult to interrupt in their raw format.

The tools in the Understand DMARC Reports subcategory help provide interpretation and quicker identification of fraudulent activity. This allows you to confidently move through the policy levels from “none”, to “quarantine”, and ultimately up to the highest level of “reject”. It is important to also consider any email organization or service authorized to send emails on your behalf, such as email marketing services, and check if they have DMARC implemented.

Only when your email domain is at “reject” will the full benefit of DMARC be realized.

6.3 Trademark Protection

Fraudsters may register domains that look very similar to your own domain in the hope that people will click through to them. Use the tools here to help identify domains that try to imitate yours, as well as domains that contain phishing or malicious content targeting your domain.

For further support while implementing DMARC refer to the **DMARC Forum** or **Protect Your Email and Reputation Category** in the GCA Community Forum.

Protect Your Email and Reputation Links:

Toolkit:

Protect Your Email and Reputation Toolbox
https://gcatoolkit.org/smallbusiness/protect-your-email-and-reputation/

Community Forum:

DMARC Forum
https://community.globalcyberalliance.org/c/dmarc/

Protect Your Email and Reputation Category
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/protect-your-email-and-reputation

Glossary of Terms

A glossary of some commonly used terms relating to cybersecurity. Some of these terms have been included in the GCA Cybersecurity Toolkit for Small Business Handbook chapters, while others are provided for additional information should you wish to explore more on your own.

account Generally refers to access to a computer system or online service, usually requiring a password to enter.

adversary An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

antivirus Software that is designed to detect, stop and remove viruses and other kinds of malicious software.

application (app) A program designed to perform specific tasks. App often refers to programs downloaded onto mobile devices.

asset A person, structure, facility, information, records, information technology systems and resources, material, process, relationships, or reputation that has value. Anything useful that contributes to the success of something, such as an organizational mission; assets are things of value or properties to which value can be assigned.

attack An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity. The intentional act of attempting to bypass one or more security services or controls of an information system.

attack signature A characteristic or distinctive pattern that can be searched for or that can be used in matching to previously identified attacks.

attack surface The set of ways in which an adversary can enter a system and potentially cause damage. An information system's characteristics that permit an adversary to probe, attack, or maintain presence in the information system.

attacker Malicious actor who seeks to exploit computer systems with the intent to change, destroy, steal or disable their information, and then exploit the outcome.

authentication The process to verify that someone is who they claim to be when they try to access a computer or online service. Also the source and integrity of data, user, process or device.

back door A covert way for cybercriminals to gain unauthorized access to a computer system

backup A copy of your data, stored in a different location than the original data, and can help you recover from an attack or data loss.

backing up To make a copy of data stored on a computer or server to lessen the potential impact of failure or loss.

bot A computer or device connected to the Internet that has been secretly compromised with malicious code to perform activities under the command and control of a remote administrator.

botnet A network of infected devices (bots), connected to the Internet, used to commit coordinated cyberattacks without their owner's knowledge.

breach An incident in which data, computer systems or networks are accessed or affected in a non-authorized way.

brute force attack Using a computational power to automatically enter a huge number of combination of values, usually in order to discover passwords and gain access.
bug An unexpected and relatively small defect, fault, flaw, or imperfection in an information system or device.

configuration The arrangement of software and hardware components of a computer system or device.

configuring The process of setting up software or devices for a specific computer, system or task

cyberattack Malicious attempts to damage, disrupt or gain unauthorized access to computer systems, networks or devices, via cyber means.

cyber incident A breach of the security rules for a system or service - most commonly; attempts to gain unauthorized access to a system and/or to data, unauthorized use of systems for the processing or storing of data, changes to a systems firmware software or hardware without the system owners consent, malicious disruption and/or denial of service.

cybersecurity The protection of devices, services and networks — and the information on them — from theft or damage.

cryptocurrency digital money. Cryptocurrency is stored in a digital wallet (online, on your computer or on other hardware. Cryptocurrency is typically not backed by any government, so does not have the same protections as money stored in a bank.

dictionary attack A type of *brute force attack* in which the attacker uses known dictionary words, phrases or common passwords as their guesses.

digital footprint A 'footprint' of digital information that a user's online activity leaves behind.

denial of service (DoS) An attack in which legitimate users are denied access to computer services (or resources), usually by overloading the service with requests.

device A piece of computer hardware that is designed for a specific function- examples include laptop, mobile phone, or printer.

DMARC Stands for Domain-based Message Authentication, Reporting and Conformance. DMARC is a mechanism that allows senders and receivers to monitor and improve protection of their domain from fraudulent email.

email domain spoofing A technique used by cybercriminals in which the "spoofed" email address used is exactly the same as the genuine one, thus making it appear to have actually been sent from that organization.

encryption Converting data into a form that cannot be easily understood by unauthorized people.

firewall A hardware/software device or a software program that limits network traffic according to a set of rules of what access is and is not allowed or authorized.

hacker Someone who violates computer security for malicious reasons, kudos or personal gain.

hardware A computer, its components, and its related equipment. Hardware includes disk drives, integrated circuits, display screens, cables, modems, speakers, and printers.

inside(r) threat A person or group of persons with the access and/or inside knowledge of a company, organisation or enterprise that could pose a potential risk through violating security policies with the intent to cause harm.

Internet of things (IoT) Refers to the ability of everyday objects (rather than computers and devices) to connect to the Internet. Examples include kettles, fridges and televisions.

intrusion An unauthorized act of bypassing the security mechanisms of a network or information system.

intrusion detection system (IDS) Program or device used to detect that an attacker is or has attempted unauthorized access to computer resources.

intrusion prevention system (IPS) Intrusion detection system that also blocks unauthorized access when detected.

keylogger Software or hardware that tracks keystrokes and keyboard events, usually secretly, to monitor actions by the user of an information system.

malvertising Using online advertising as a delivery method for malware.

malware (malicious software) a term that includes viruses, trojans, worms or any code or content that could have an adverse impact on organisations or individuals. Software intended to infiltrate and damage or disable computers.

mitigation The application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences.

network Two or more computers linked in order to share resources.

outside(r) threat A person or group of persons external to an organization who are not authorized to access its assets and pose a potential risk to the organization and its assets.

password A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

password crackers Programs designed to guess a password, often by cycling through commonly used combinations or using a username and password obtained from an account that suffered a breach.

password managers Programs that allow users to generate, store and manage passwords in one location securely.

patching Applying updates to firmware or software to improve security and/or enhance functionality.

pentest (penetration testing) An authorized test of a computer network or system designed to look for security weaknesses so that they can be fixed.

Personal Identifying Information / Personally Identifiable Information (PII) The information that permits the identity of an individual to be directly or indirectly inferred.

pharming An attack on network infrastructure that results in a user being redirected to an illegitimate website despite the user having entered the correct address.

phishing Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website. A digital form of social engineering to deceive individuals into providing sensitive information.

plaintext Unencrypted information.

proxy server Server that acts as an intermediary between users and others servers, validating user requests.

ransomware Malicious software that makes data or systems unusable until the victim makes a payment.

recovery The activities after an incident or event to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.

resilience The ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.

restore The recovery of data following computer failure or loss.

risk assessment The process of identifying, analysing and evaluating risk along with the potential harmful consequences for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.

security information and event management (SIEM) Process in which network information is aggregated, sorted and correlated to detect suspicious activities.

smishing Phishing via SMS - mass text messages sent to users asking for sensitive information (eg bank details) or encouraging them to visit a fake website.

signature A recognizable, distinguishing pattern. Types of signatures would include: attack signature, digital signature, electronic signature.

social engineering Manipulating people into carrying out specific actions or divulging information that is of use to an attacker.

software Refers to programs for directing the operation of a computer or processing electronic data.

spam The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

spear-phishing A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.

spoofing Faking the sending address of a transmission to gain illegal [unauthorized] entry into a secure system. Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing.

spyware Malware that passes information about a computer user’s activities to an external party.

supply chain A system of organizations, people, activities, information and resources, for creating and moving products including product components and/or services from suppliers through to their customers.

system Generally refers to a system of one or more computers or devices that input, output, process, and store data and information.

system administrator (admin) Person who installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability; also manages accounts, firewalls, and patches; responsible for access control, passwords, account creation and administration.

threat Something that could cause harm to a system or organization.

threat actor An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

trojan (trojan horse) A computer program that is disguised as legitimate software but with a hidden function that is used to hack into the victim's computer. A type of malware.

two-factor authentication (2FA) The use of two different components to verify a user's claimed identity. Also known as multi-factor authentication.

virtual private network (VPN) An encrypted network often created to allow secure connections for remote users, for example in an organisation with offices in multiple locations.

virus A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer. A type of malware

vulnerability A weakness, or flaw, in software, a system or process. An attacker may seek to exploit a vulnerability to gain unauthorized access to a system.

whaling Highly targeted phishing attacks (masquerading as legitimate emails) that are aimed at senior executives.

worm A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. A type of malware

Definitions compiled from resources produced by:

British Standards Institute
https://www.bsigroup.com/en-GB/Cyber-Security/Glossary-of-cyber-security-terms/

National Cyber Security Centre (NCSC -UK)
https://www.ncsc.gov.uk/information/ncsc-glossary

National Initiative for Cybersecurity Careers and Studies (NICCS -US)
https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary

Additional Resources:

Australian Cyber Security Centre Glossary
https://www.cyber.gov.au/acsc/view-all-content/glossary

Global Knowledge
https://www.globalknowledge.com/us-en/topics/cybersecurity/glossary-of-terms/

SANS Institute Glossary of Security Terms
https://www.sans.org/security-resources/glossary-of-terms/