It is unimaginable for any business today to function without using any form of technology. But along with technology comes the risk of your equipment being exposed to cyberattacks and your information being compromised. These attacks can be prevented by startups, whether big or small, by having a security-first mentality. Businesses that understand these threats can avoid these cyber-attacks which can otherwise disrupt their operations and cause mistrust among customers and clients. However, startups often utilize their resources in other business areas such as sales and operations that mostly overlook the security part of your business. This is why, it is important for startups to know the importance of cyber security for their business.

Here are 10 things business startups and entrepreneurs need to know about cyber security.

1. **People are often the Weakest Link**

Even trustworthy employees cannot guarantee protection of your network. Often, it only takes a lapse in judgement to give away network access to a hacker. Cyber criminals use phishing attack to trick honest employees into clicking malicious links and give away their sensitive information. In some instances, employees unknowingly compromise business data by connecting their compromised devices to the organization’s network.

The only way to avoid this is by training and educating your employees. Teach them how to identify and avoid the threats to decrease the chances of human error. Also devise information security policy that guides how the staff should be using their IT equipment. Teach your employees about password best practices and also train them to recognize phishing and social engineering attacks. They should know to check the sender’s email address, format and name, especially in case of an unexpected request. Before clicking any link in an email, make sure that it came from a trustworthy source or otherwise don’t open it. If an email asks for an information, make a phone call to the sender first to cross check its authenticity.

1. **Access Control Matters**

You need to know who has access to your infrastructure. As a business startup, when you initially launch, you may have handed out critical information to third-party vendors or other stakeholders. You may still have given access of your servers to an ex-employee who has already left the job a month ago. It is important that when your relationships change with any entity, you revoke the access privilege granted to them.

Most software tools now allow businesses to set up user access with different control levels for different users. These tools can allow employers to restrict entry locations for employees and set different levels of security for their convenience and safety. If and when an employee has left the company, they can be prevented from gaining unauthorized access by deactivating their profile. You can also keep a track of who enters your premises, and what are their entry doors that they use. These systems can also alert you in case an employee is found present in an area where they do not belong.

Even for those who have access to highly sensitive content, encourage them to use strong passwords. Also, to ensure legal obligations, make your stakeholders sign non-disclosure agreements when involving them in any business matters.

1. **Invest in Security Software**

Most startups are low on budget and may be hesitant to take on any added expense. However, investment in cybersecurity is one investment you should not ignore. In fact, even with the low budget you can still invest in cost-effective antivirus, firewall and encryption utilities. Additionally, with security-as-a-service as a new thing, now you don’t need to make heavy investments in security applications for your network’s protection. Rather, you can subscribe to web applications that fulfill all your basic security needs. You can pay a monthly nominal fee instead of purchasing the complete software. In return, the service provides complete protection of your data, apps and operations that run in the cloud.

Consider, if you don’t invest in a software service, your business may suffer from data loss, compromised credentials, hacked APIs, Denial of Service Attacks, violation of regulatory compliance, Advanced persistent threats, hijacked traffic and many other threats. With a security as a service, you can overcome these without paying hefty amounts or exhausting your IT resources as most of these services integrate with your existing infrastructure.

1. **Small and Large Businesses are Equal for Cybercriminals**

It is normal to believe that hackers only target big businesses and high-profile startups. However, according to a [study](https://www.ponemon.org/blog/smbs-are-vulnerable-to-cyber-attacks) by Ponemon institute, about 55 percent of small and medium businesses have experienced cyberattacks in some form. Regardless of the size of your business, most cyberattacks are now caused by malicious scripts and software programs. Moreover, if you are a small business, you are more likely to be a target due to your lack of experience and limited knowledge of cyber security. Therefore, any business that has a digital presence is vulnerable to threats. Even if you are a small business, you need to take security seriously and take all the measures as a big organization would.

1. **Data Breaches**

Hackers can compromise your data in several ways. But the top concern is a data breach. A data breach occurs when an attacker gains access to your database and steals your sensitive data. He then sells your personal or financial information in the black market which can be used for online fraud and identity thefts. Main targets of such attacks are ecommerce or online support websites that store customer information such as [credit card data](file:///E:\Upwork\Cardzgroup\Unpaid\cardzgroup.com). Small startups can definitely not afford to lose their customer’s trust as they don’t have all the resources to resurface after a stained reputation.

As in many other cases, data breaches are often a result of employee negligence. To prevent your business from potential data breaches, you need to limit access to your valuable data. When you put a limit to who can view customer’s financial information, you narrow down the number of employees who may accidentally click on a phishing link. You may be sure about your employees taking all the measures, but you cannot say the same for your third-party vendor employees. Hence, businesses need to ensure to limit the type of documents their third-party vendors can view. Also create a risk mitigation or breach response plan for a proactive response in case of an actual breach.

1. **Malware and Ransomware**

Ransomware is a specific malware which infects a system by encrypting the important files in it and then asking the owner to pay a ransom amount in exchange of being able to access their encrypted files. It is considered as one of the top threats for startups today. Cybercriminals demand handsome amounts of money in exchange of decrypting the owner’s files and usually ask for payment in cryptocurrencies due to the nature of anonymity in the payment method. This not only causes businesses to suffer from financial losses but also results in business disruption for an indefinite time period.

Contrary to popular belief that only established businesses face ransomware attacks, startups are equally at risk because of being an easy prey. This is because new businesses spend lesser on employee training and security software and are easy targets. Many of them don’t have the right technology to detect ransomware and once infected, they don’t have a complete system backup. This causes them to typically pay for the ransom to recover the data. In fact, it is this willingness of paying which makes startups an attractive target. While hackers may not demand the same large ransom amounts as they do from large organizations, they can still get a large payoff by attacking multiple startup businesses.

1. **Distribute Denial-of-Service Attack**

These kinds of attacks make your website inaccessible by others by purposely increasing traffic on your network. It involves hijacking and infecting multiple devices with malware, and then using them to overwhelm a service, website or server with incessantly high fake traffic resulting in its disruption. For a one- or two-hour website downtime, a business can suffer huge financial losses. Most businesses know that even only a few minutes of downtime proves causes severe damage to the company’s reputation and results in decreased customer confidence.

To prevent DDoS attacks, startups can use services such as Cloudflare or Akamai which provide DDoS protection, web app firewalls, cloud networking and cloud optimization tools among other features.

1. **Compliance to Security Standards**

Security standards such as General Data Protection Regulation (GDPR) and ISO 27001 serve to provide security guidelines for businesses to keep them safe from information security troubles.

It is advisable to comply with these standard regulations early on in your business to not only gain recognition among your clients but also ensure that your safety practices are in place. You will also avoid spending countless money and time on mitigating risks and responding to threats faced later. Furthermore, startups that are ISO certified have better chances of working with large companies and government departments, due to security compliance often being a prerequisite.

1. **Web Security Management**

If you are a startup that actively depends on a website to run its operations, such as an ecommerce store or an online healthcare startup, make sure to secure your website by getting SSL certificates installed.

SSL or Secure Sockets Layer is a security technology of global standard which allows encrypted communication between a web server and browser. It greatly decreases the risk of leakage of sensitive information such as passwords and credit card information. In essence, it allows a private conversation between two parties by authenticating the website and encrypting the data being transmitted. This protects your website from hacking attempts being successful and keeps customer data secure.

1. **Limit Your Digital Footprints**

As startups use a number of business and mobile applications for effective management of their businesses, each person or business entity may have multiple accounts ranging from emails, social media, and software applications. This can lead users to use the same password for multiple accounts, either with the fear or forgetting different passwords or out of laziness. To limit your digital footprints, don’t share accounts, use multifactor authentication where available, keep different passwords for all accounts and close all unused accounts.

**Final thoughts**

For business startups, cyber security is a phenomenon which does not directly affect their goals. Nevertheless, its importance cannot be ignored as it is very necessary in today’s ever evolving digital world.