CYBER SECURITY 101

What Your SMB Should Know

CYBERSECURITY 101

Cyber attacks occur daily. More than half (55 percent) of SMBs and Mid-Market companies with fewer than 1,000 employees have experienced a cyber attack, while 43 percent of all attacks target small businesses. Hackers seek companies that carry information with a dollar value. This includes medical records, credit card information, Social Security numbers,

When it comes to starting a small to medium sized business, new owners have many decisions to make and often leave cybersecurity measures by the wayside. A daunting static was released by U.S. National Cyber Security Alliance that stated "60% of all SMBs fail within six months of a cyberattack." The "I don't have anything worth stealing" mentality ends up leaving points of entry wide open for hackers. The reason hackers target SMBs is due to them having more digital assets to target than an individual consumer has but less security than an larger enterprise.

Since security breaches can be devastating to a SMB, owners are more likely to pay a ransom to get their data back. SMBs can merely be a steppingstone for attackers to gain access to larger businesses. It is important for SMBs to understand the threats and learn strategies to help protect them.

STAY INFORMED

UNDERSTANDING THE THREATS

To break into your company, a hacker is going to most likely use one of these methods:

- **Ransomware:** Malware that locks computers and encrypts data, preventing businesses access, often until ransom is paid.
- **Phishing:** Entices users to click an email or attachment containing a virus that then infects their computer, and possibly other machines.
- **Malvertising:** Short for "malware advertising," it consists of delivering malware to a network after a user clicks on an apparently legitimate advertisement.
- **Clickjacking:** Hiding hyperlinks to compromised web pages in website links where users reveal personal data, which is then stolen.
- **Drive-by-downloads:** A dirty trick that downloads malware into networks. Sometimes from a pop-up window or even a compromised website.

OBTAIN KNOWLEDGE

CYBERSECURITY MYTHS

There are several misunderstandings when it comes to SMBs cybersecurity. Even in 2020, many SMB executives still believe their companies are not exposed to the same cyber threats that large companies recognize. These are the four most common cybersecurity myths amont SMB's:

Myth: We don't have anything a cyber criminal would want

Cybercriminals are after something simple and that is profit. They are not too concerned with where the money comes from, they just need to make sure it keeps coming in. If you have store your customers personal information including credit cards, banking info, SSN, etc, then you have what a cyber criminal would want.

Myth: We're too small to be a target for cyber criminals

Two thirds of SMB's have suffered a cyber attack in the last 12 months. If your business was not targeted in 2019, consider yourself lucky. You were in the minority or worse, a successful breach has yet to be detected. You are never too small for cyber criminals to target.

Myth: Our company can't afford to invest in cybersecurity

83% of SMBs lack the funds to deal with repercussions of a cyber attack. This means a single attack can cause them to shut their doors for good. An individual cyber attack has been reported to average $3 million in damages. Just think, is this something you could afford happen to you?

6 BEST PRACTICES

Follow these 6 best practices so your business doesn't become another statistic

1. **Set a Strategy**
   Understand the threats and what cyber criminals are after in order to build up your defenses.

2. **Educate Users**
   Train employees to turn them into the front line of defense. Uninformed workers can lead to risk.

3. **Apply Advanced Tools**
   Acquire tools that deliver endpoint protection, secure the network through firewalls, and perform threat analysis.

4. **Maintain a Firewall**
   Use a firewall to create a barrier that determines which content to allow into your network and which to block.

5. **Strengthen Password Management**
   Change passwords regularly and be sure to use combinations that are harder to crack than commonly used words.

6. **Implement Backup and Recovery**
   Failure to backup data exposes a company to disaster because if you suffer a data loss, that data is gone forever. It also puts companies in a very weak position if struck by ransomware.

PROTECT
YOUR DATA

TDS NETWORKS