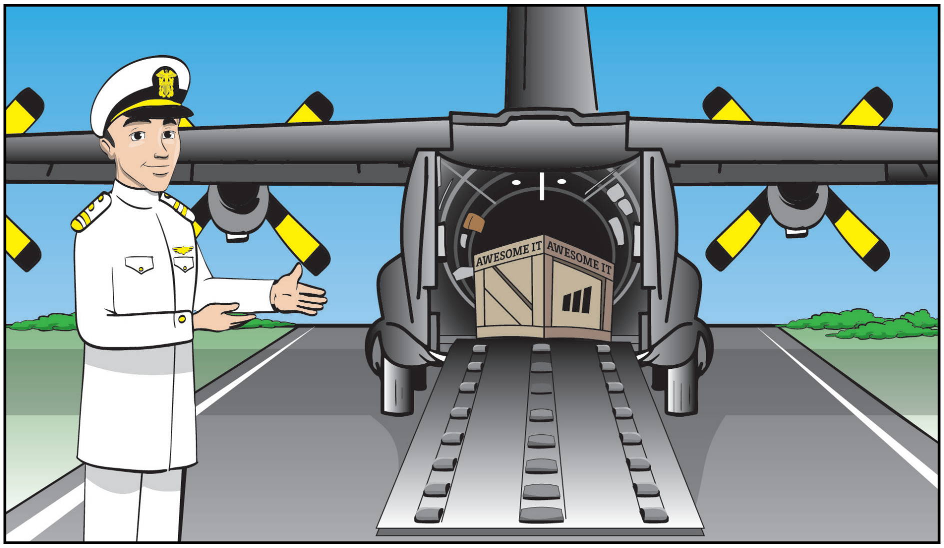
Tier 3 Technology Solutions June 2023

ISSUE #1

Tier 3 TechTips

Your Monthly Guide to the Latest Tech Tips & News



WELCOME TO TIER 3 TECHNOLOGY'S NEW MONTHLY NEWSLETTER!

Well, here we are. There were some hiccups, but we finally made it. We have a newsletter. It was a long and winding road.

First, we tried to make it big on primetime TV, only to be politely informed by a very nice television executive that we have what is known in the business as "faces for radio."

Radio executives agreed but then regretfully informed us that the sound quality of our voices was more suited for print.

So here we are! The very first issue of our new monthly newsletter! Every month, we'll bring you all the tech tips, news, and best practices we can get our hands on. And we'll try our best to accomplish that in a non-boring way.

We're still holding out hope for TV, though. Maybe something in the 2 am slot on public access...?

Until then, we hope you enjoy our new monthly newsletter. We enjoyed putting it together for you.

— The Team at Tier 3 Technology Solutions

Newsletter Highlights

TIER 3
TECHNOLOGY
Managed IT Services
& Security Solutions

THE DARK WEB TOTALLY SUCKS: WHY SMALL BUSINESSES ARE AT RISK

The dark web, also called the darknet, contains websites and content not available on the surface web, including illegal marketplaces, forums, and other websites related to criminal activities.

It is not indexed by traditional search engines and offers anonymity and encryption to its users, making it an attractive and low-risk option for cybercriminals trafficking stolen data.

While the dark web is notorious for being a breeding ground for criminal activities like drug trafficking and arms sales, it also poses significant risks beyond these well-documented crimes.

Cybercriminals use the dark web as a marketplace to sell stolen data, and all organizations are at risk — even (maybe especially) organizations who believe they're too small or don't "have data worth stealing."

Personal information like names, addresses, phone numbers, birthdates, emails, usernames, passwords, social security numbers, credit card numbers, and bank account details are all in high demand on the dark web.

While cybercriminals can use this information for identity theft or financial fraud, it's sometimes simpler and more lucrative to package it for sale on the dark web. Modern cybercriminals know that breaching a network, even that of a small business, is worth the effort.

Many hackers are targeting small businesses because they're easier targets.

Why are small businesses easier targets? It's not their size. They're easier targets precisely because many don't believe they're worth targeting and, as a result, underinvest in cybersecurity.

An initial security breach often goes unnoticed; a full attack may not come for weeks or months. Hackers plant malicious software that allows them to collect data over an extended period and use the gathered information for more complex attacks. For instance, hackers may use phishing emails to access a user's computer; once they have access, they can use spyware to track key inputs, enabling them to mine passwords. They use this data for a direct attack like Ransomware or package all the information they have gathered for sale on the dark web.

Personal information is in high demand right now on the dark web.

The dark web is a hidden part of the internet that poses significant risks to small businesses — and offers excellent incentives (and low risk) for threat actors targeting small organizations.

EFFECTIVE 2FA APPS YOU CAN EASILY IMPLEMENT TODAY

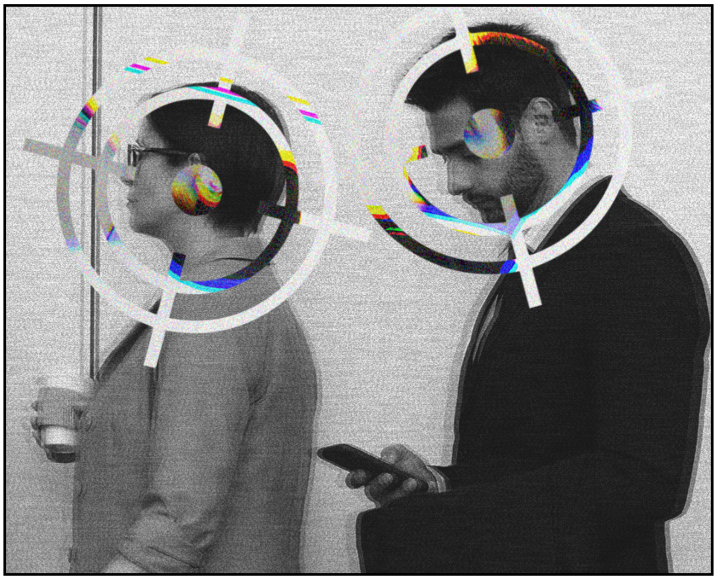
Two-factor authentication (2FA) is an important (and simple) security measure. With 2FA, users must provide two types of authentication to access their account—usually a password and a one-time code. This makes it much harder for hackers to access your account, even if they obtained your password through a data breach or other means.

1. **Google Authenticator:** A free app that generates codes for two-factor authentication

2. **Microsoft Authenticator:** A free app that supports multi-factor authentication.

3. **Authy:** A free app that supports two-factor authentication for many popular online services.

4. **LastPass Authenticator:** A free app that provides extra security for LastPass users.
All of these are available on Android and iOS.



4 METHODS HACKERS USE TO PICK A TARGET

According to Astra Security, in 2023 we'll see an estimated 33 billion account breaches. That's 33 billion *successful* account breaches — not attempts. Hackers have a busy year ahead.

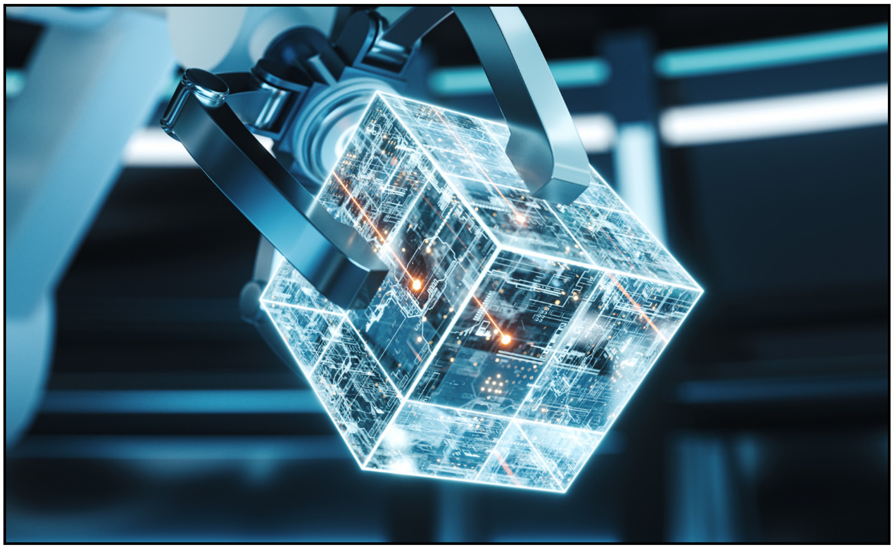
But how are they choosing their targets?

1. **Vulnerability scanning:** Hackers use automated tools to scan the internet for vulnerabilities like outdated software or weak passwords.

2. **Social engineering:** Hackers use social engineering techniques to trick individuals into giving them access to their systems. Phishing is the most widely used form of social engineering.

3. **Industry or sector targeting:** Hackers target specific industries or sectors more likely to have valuable data or weak security controls. For example, healthcare/financial services and small businesses are ideal targets.

4. **Random selection:** Often, hackers do not have any specific target in mind and will focus on building automated systems that attack anyone with an online presence.



LET'S DEBUNK SOME OF THE MOST COMMON CYBERSECURITY MYTHS

Cyberattacks have exploded in recent years and continue to increase in frequency. The sophistication of hackers and their tools is evolving daily, and the attack surface created by the proliferation of internet-connected devices continues to broaden.

In other words, if stealing data is your business, business is booming. It's only natural, then, that cybersecurity has become an increasingly important (and noticeable) part of our daily lives.

As the public becomes more aware of an issue (in this case, cyberattacks), myths and misconceptions will germinate and spread. Cybersecurity is no exception.

As a result, there are plenty of misconceptions regarding cybersecurity out there. Here are four of the most common cybersecurity myths we regularly encounter.

Myth: Only big companies need to worry about cybersecurity.
FACT: Cybercriminals target small businesses just as frequently as larger ones. This myth is commonly repeated, and it's a particularly harmful one.

Myth: Antivirus software is enough to protect against all cyber threats.
FACT: Antivirus software is just one layer of protection and is insufficient to protect against all cyber threats. Security measures like Next-gen firewalls, regular software updates, and team member training are crucial for maintaining a secure environment.

Myth: Cybersecurity is just an IT issue.
FACT: Cybersecurity is a companywide issue that involves everyone from the CEO to summer interns. All team members should be able to identify and report potential threats and maintain good cybersecurity practices.

Myth: Cybersecurity breaches only originate from external sources.
FACT: The term **insider threat** in cybersecurity refers to the risks posed by individuals or entities with authorized access to an organization's sensitive or confidential data, systems, or networks. It's essential to have measures to protect against insider threats, like the principle of least privilege (POLP) or network segmentation.

Are You Ready to Take the Next Step?

Start the Conversation! We're eager to get to know you, discuss your vision and goals, and even provide you with a free 15-minute consultation. Learn more at GoTier3.com.

"They feel like part of our work family. They're not just invested in our network, but in the growth of our firm and making sure that the system we use fosters that growth."
~ Kelly Beattie, Beattie Law Firm

TIER 3 TECHNOLOGY