ISSUE 21 FALL 2019

RJ2 TECHNOLOGIES

Newsletter

What's Inside

October is Cybersecurity Awareness Month!

What is cybersecurity?
It seems that everything relies on computers and the internet now—communication (e.g., email, smartphones), entertainment (e.g., digital cable, mp3s), transportation (e.g., car engine systems, airplane navigation), shopping (e.g., online shopping, credit cards), medicine (e.g., medical equipment, medical records), and the list goes on. How much of your daily life relies on computers? How much of your personal information is stored either on your own computer or on someone else's system?

Cybersecurity involves protecting that information by preventing, detecting, and responding to cyber attacks.

What are the risks to having poor cybersecurity?
There are many risks, some more serious than others. Among these dangers are malware erasing your entire system, an attacker breaking into your system and altering files, an attacker using your computer to attack others, or an attacker stealing your credit card information and making unauthorized purchases. Unfortunately, there's no 100 percent guarantee that even with the best precautions some of these things won't happen to you, but there are steps you can take to minimize the chances.

What can you do to improve your cybersecurity?
The first step in protecting yourself is to recognize the risks and become familiar with some of the terminology associated with them.

Hacker, attacker, or intruder - These terms are applied to the people who seek to exploit weaknesses in software and computer systems for their own gain. Although their intentions are sometimes fairly benign and motivated solely by curiosity, their actions are typically in violation of the intended use of the systems they are exploiting. The results can range from mere mischief (creating a virus with no intentionally negative impact) to malicious activity (stealing or altering information).

Malicious code (Malware) - Malicious code, also called malware, is a broad category that includes any code that could be used to attack your computer. Malware can have the following characteristics:
It might require you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular webpage. Some forms of malware propagate without user intervention and typically start by exploiting a software vulnerability. Once the victim computer has been infected, the malware will attempt to find and infect other computers. This malware can also propagate via email, websites, or network-based software. Some malware claims to be one thing, while in fact doing something different behind the scenes. For example, a program that claims it will speed up your computer may actually be sending confidential information to a remote intruder.

Examples of malware include: viruses, worms, and ransomware.

Vulnerabilities - Vulnerabilities can be caused by software programming errors. Attackers may try to take advantage of these errors to infect your computer, so it is important to apply updates or patches that address known vulnerabilities.

Safe Guarding Your Data

Why isn't "more" better?
Maybe there is an extra software program included with a program you bought. Or perhaps you found a free download online. You may be tempted to install the programs just because you can, or because you think you might use them later.

These risks become especially important if you use your computer to manage your personal finances (banking, taxes, online bill payment, etc.), store sensitive personal data, or perform work-related activities away from the office. However, there are steps you can take to protect yourself.

How can you protect both your personal and work-related data?

- ***Use and maintain anti-virus software and a firewall –*** Protect yourself against viruses and Trojan horses that may steal or modify the data on your own computer and leave you vulnerable by using anti-virus software and a firewall. Make sure to keep your virus definitions up to date.
- ***Regularly scan your computer for spyware –*** Spyware or adware hidden in software programs may affect the performance of your computer and give attackers access to your data.
- ***Keep software up to date*** – Install software patches so that attackers cannot take advantage of known problems or vulnerabilities.
- ***Evaluate your software's settings*** – The default settings of most software enable all available functionality. However, attackers may be able to take advantage of this functionality to access your computer. It is especially important to check the settings for software that connects to the internet (browsers, email clients, etc.).
- ***Avoid unused software programs*** – Do not clutter your computer with unnecessary software programs. If you have programs on your computer that you do not use, consider uninstalling them. In addition to consuming system resources, these programs may contain vulnerabilities that, if not patched, may allow an attacker to access your computer.
- ***Establish guidelines for computer use*** – If there are multiple people using your computer, especially children, make sure they understand how to use the computer and internet safely. Setting boundaries and guidelines will help to protect your data.
- ***Use passwords and encrypt sensitive files*** – Passwords and other security features add layers of protection if used appropriately. your passwords and passphrases; if you forget or lose them, you may lose your data.
- ***Follow corporate policies for handling and storing work-related information*** – If you use your computer for work-related purposes, make sure to follow any corporate policies for handling and storing the information. These policies were likely established to protect proprietary information and customer data, as well as to protect you and the company from liability.
- ***Follow good security habits –*** Review other security tips for ways to protect yourself and your data.

FEATURED PARTNER

ID AGENT

ID Agent provides a comprehensive set of threat intelligence and security training solutions to private and public-sector organizations and to millions of individuals impacted by cyber incidents.

Call RJ2 for your FREE Dark Web Scan!

RJ2 SPOTLIGHT

Eric Schreiber

Manager of Client Services

Eric Schreiber is responsible for managing the high level of support that RJ2 Technologies' provides to our clients. He has a passion for increasing the satisfaction of RJ2 Technologies' clients by developing effective methods to increase the efficiency of the support team. Prior to joining RJ2 Technologies, Eric was the IT Manager for a large Volvo Construction dealership.

Fun Fact: Eric enjoys spending time with his family, watching sports, and being an active member with his alma mater's football team.

BUSINESS PRESENCE

What is the Right Cloud for You?

***Businesses around the globe have** been moving toward the cloud and are reaping the benefits of continuity, data security, and process efficiency. However, with more data comes more responsibility. This means that you'll need to find the right kind of service that's suitable to the infrastructure you have. Fortunately, various cloud management tools and solutions are available in the market. Let's take a closer look.*

1. SOFTWARE-AS-A-SERVICE (SAAS)

Easily the largest and most well known cloud-based service, SaaS uses the cloud to deliver apps to users, and these apps are then usually accessed via a web browser. This means users who have access to the internet can access the software from any device, at any time. Unlike physical software that you install on your computer, SaaS solutions are hosted on a provider's servers. In a nutshell, SaaS is:

Available over the internet
Hosted on a remote server by a third-party provider
Scalable, with different tiers for small, medium, and enterprise-level businesses
Inclusive, offering security, compliance, and maintenance as part of the cost

With SaaS, your provider is responsible for software maintenance and updates, which means users will all be using the same version of software and get updates at the same time. As a business owner, this means that managing the software on all of your computers is not only easier, but more affordable.

SaaS software solutions include office document creation suites, accounting software, email, HR solutions, content management, customer relationship management (CRM), and more.

2. PLATFORM-AS-A-SERVICE (PAAS)

PaaS is primarily used by developers who need a virtual environment for developing and testing their own custom software or applications. This means developers don't need to build and maintain their own infrastructure (which is comprised of networking devices, storage, servers, an operating system, and other necessary hardware and software) from scratch when developing applications, saving the firm time and money. Most companies who utilize PaaS do so to either host or develop their own software solutions, or to provide support for software used by employees. PaaS platforms are:

Accessible by multiple users
Scalable — you can choose from various tiers of resources to suit the size of your business
Built on virtualization technology
Easy to run without extensive system administration knowledge

While PaaS is gaining in popularity with many small businesses, most won't have firsthand interaction with this type of cloud because they won't need to build their own software or app.

3. INFRASTRUCTURE-AS-A-SERVICE (IAAS)

IaaS offers services such as pay-as-you-go storage, networking, and virtualization. The most popular and well-known type of IaaS is the virtual machine — a digital version of a computer or server that is accessed over an internet connection. IaaS gives users cloud-based alternatives to expensive on-premises infrastructure so businesses can use their funds to invest in other things.

In other words, if you are looking to virtualize your systems via the cloud, IaaS is a good place to start, as it allows you to move existing support systems into the cloud. Other solutions can then be migrated or introduced as needed. IaaS is essentially:

Highly flexible and scalable
Accessible by multiple users
Cost-effective

While the cloud offers a wide variety of benefits and solutions, choosing the service which is best for your company's needs can be tedious. To ease this burden, get in touch with us today. We'll help you find the best solution your business needs and ensure proper migration and implementation so you can focus on running your business.

Featured Product:

Dark Web ID

Dark Web ID™ is the leading Dark Web monitoring platform in the Channel.

The award-winning platform combines human and sophisticated Dark Web intelligence with search capabilities to identify, analyze and proactively monitor for an organization’s compromised or stolen employee and customer data.

More Managed Service Providers globally rely on Dark Web ID than any other monitoring service to provide actionable stolen credential data. Trust the leader in the Channel.

October

"The most technologically efficient machine that man has ever invented is the book."
-Northrop Frye

Tech Tips of the Month:

1. Use strong passwords to prevent a hacker from stealing your information.

2. If it looks stetchy DO NOT CLICK ON IT!

3. Always make sure your anti-virus software is up to date. Hackers are always creating new mega-viruses.