Popular Article

Safe Space: An Introduction to Cybersecurity

Janet Campbell

Elderspark.com

Cybersecurity is a complicated field but one that is increasingly pertinent to businesses operating in the digital space. Today, Biotechnology Kiosk explores precisely how cybersecurity works and what can be done to protect sensitive information online.

What Is Cybersecurity?

In a nutshell, cybersecurity is the protection and maintenance of computer systems/networks against theft, damage, or disruption. The need to secure our personal information, intellectual property, and critical data runs parallel to our increased dependence on technology. As politics and business grow increasingly entwined with digital applications, so do threat actors multiply with the aim to infiltrate and disrupt our flow of data and money.

For all these reasons, it's good to have someone on your staff (perhaps you yourself) who is well-acquainted with cybersecurity and how to implement it. If you've ever thought about going back to school, this may help protect your business and be well-worth it in the long run – especially if you take advantage of online learning platforms that allow you to work remotely and learn at your own pace.

Identifying Risk

Larger businesses tend to have specialized personnel (such as Chief Information Security Officers) to oversee and strategize against cybersecurity risks. In the absence of an expert, it's up to the business owners themselves to read up, identify risks and prepare for a potential attack. This begins with:

- Documentation of systems, applications, and information in company use with an aim to ensure confidentiality, integrity, and availability at all times.
- Pre-established risk management frameworks that are applicable to your existing systems.
- A framework aimed to identify, document, and manage attacks (written in expectation of and prior) in relation to existing systems and applications.

To help with this, it makes sense to familiarize yourself with the various risks posed to your business in relation to your digital practices, systems, and applications.

Preparing Systems

Implementing the protocols that can protect against an aggressor is essential to help avoid or defend against a potential breach.

- Systems and applications should be delivered (and maintained) by trusted suppliers only.
- Personnel should be available to understand and secure any vulnerabilities in systems/applications.
- There should be pre-existing rules that ensure only trusted, supported operating systems, applications, and computer code are used on company hardware and databases.
- Information should be encrypted at all times, including during transit between systems - this information should also be inspectable, controlled, and auditable.
- Everything should be backed up.
- Only trusted, qualified personnel should be granted access to systems, applications, and sensitive data repositories - this exposure should be limited whenever possible, and authentication should be used.
- Team members should be familiar with basic cybersecurity practices.
- Physical access to systems should be restricted to authorized personnel only.

With comprehensive preparatory controls, you can reduce the possibility of an attack and limit any damage should a breach occur.

Detecting Threats

You can't react to an attack if you don't know when one is occurring. In order to detect and analyze threats, it's important to use the relevant tools and applications.

- Firewalls are designed to block unauthorized access to your computer system/network
- An Intrusion Prevention System (IPS) regularly monitors your network for any malicious activity and can be programmed to prevent it by reporting, blocking, or destroying threats.
- An Endpoint Detection and Response System (EDR) monitors and collects activity data that might indicate a threat, automatically responds to identified threats and, using advanced technology, provides a forensic analysis for use by security personnel.

Responding to Attacks

A security breach is certain to negatively impact a business. This could mean damage to the brand image, lost revenue, reduced productivity or even legal implications.

- Ensure that any incidents are identified and reported both internally and externally to any relevant bodies. Speed is of the essence.

- Incidents should be contained, eradicated and recovered from as quickly as possible. Hesitancy in the event of an attack can prove damaging.
- Recovery/continuity plans should be enacted to help mitigate damage.

Companies or business entities that fail to protect themselves from cyber threats are the ones most likely to be targeted by them. By taking the necessary steps today, it's possible to reduce the likelihood of a breach and mitigate the damage should one occur.

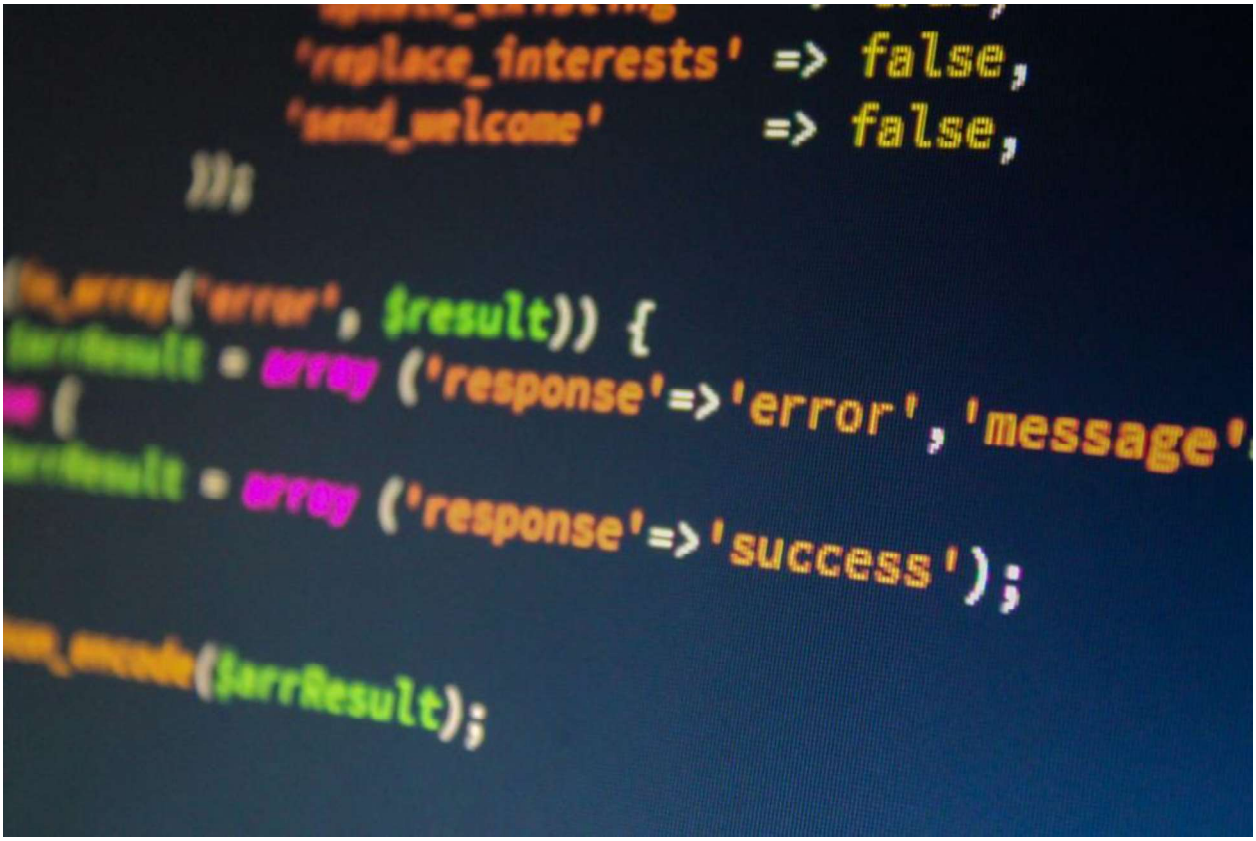

Image by Pexels

***Biotechnology Kiosk** was founded in May, 2019 by Dr. Megha Agrawal and Dr. Shyamasri (Shya) Biswas to serve the global biotechnology and medical science community. If you have any questions, please email publisher@biotechkiosk.com.*