DO YOUR PART, #BECYBERSMART

Proactive Tips for Keeping Your Data Secure

This National Cyber Awareness Month, let's take a look at how cyber threats have changed and discover ways to protect our data, assets, and organizations in this new digital world.

The Rising Threat of Cyber Attacks

$6 Trillion

the predicted cost of cyberattacks on global markets in 2021[1]

Since the start of the pandemic:

300%

Reported cyberattacks have increased by **300%** according to the FBI.[2]

3x

Employees are clicking on **three times** as many malicious emails as they had before.[3]

Phishing was the most common type of cybercrime in 2020 with **over 90%** of attacks occurring over email.[4]

In 2021, the average ransomware payment **increased by 82%** year over year to $570,000.[5]

80% of companies who had a data breach could have prevented it by patching and updating on time, according to one survey.[6]

Personal computers without antivirus software are, on average, **5.5 times** more likely to be infected.[7]

A 2019 report from Microsoft concluded that multi-factor authentication **blocks 99.9%** of automated attacks.[8]
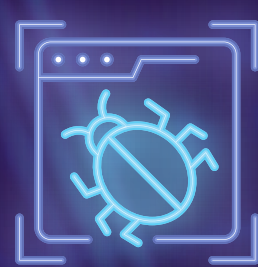
40%

of data loss is caused by hardware failure. 140,000 hard drives crash every week in the United States.[9]

Tips for Staying Safe, The Importance of Proactive Prevention

Proactive prevention is the best defense against the growing tide of cyber threats. Many of these threats can be prevented with simple security measures. By taking the time to implement these tips, you can protect yourself and others, ensuring all of your data remains safe from malicious actors looking to exploit it.
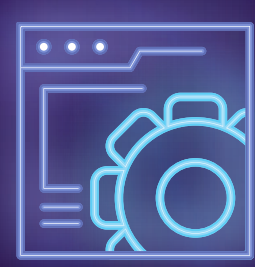
- Keep your software up to date
- Download antivirus software
- Use strong passwords
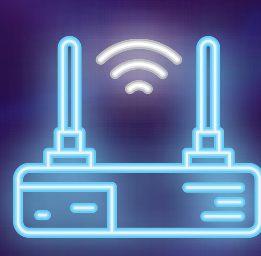- Use two-factor or multi-factor authentication
- Regularly check online accounts and credit reports
- Secure your mobile device
- Protect your sensitive personal identifiable information (PII)
- Avoid public Wi-Fi
- Backup data

Do Your Part, #BeCyberSmart

[1] CisoMag – [2] The Hill – [3] Mimecast – [4] Federal Bureau of Investigation – [5] Palo Alto Networks
[6] eWeek – [7] Safety Detectives – [8] Microsoft – [9] Hosting Tribunal

Dictionary

Phishing	A type of attack where criminals send fraudulent messages designed to trick a victim into revealing sensitive information such as passwords or banking details.
Ransomware	A malicious computer program that holds your data and privacy hostage in exchange for money.
Multi-factor authentication	When a service requires an extra security layer—such as a phone number or email confirmation — in addition to username and password.