IN A WORLD OF BAD ACTORS, #BETHECYBERSTAR

Proactive Tips for Keeping Your Data Secure

Let's take a look at how cyber threats continue to grow exponentially as well as the best practices for protecting your data, assets, and organizations.

The Cost of Cybercrime Continues to Climb

$10 Trillion the predicted cost of cyberattacks on global markets by 2025.[1]

Susceptibility to Attack Methods is Growing

In 2022, the Internet Crime Complaint Center (IC3) received

21,832 complaints

totaling more than **$2.7 billion in losses** from business email compromise (BEC) schemes, an evolution of simple hacking or phishing that target both businesses and individuals performing transfers of funds.[2]

At least one known open-source vulnerability was detected in 84% of all commercial and proprietary code bases in 2022, **up 4% from 2021.**[3]

In 2023, **80% of reported cybercrimes** were attributed to phishing attacks.[4]

Threat actors are increasingly using AI to craft more sophisticated phishing campaigns, including large language model (LLM) generated emails, deep fakes, and voice cloning technology to impersonate family, friends, and colleagues.[5]

In 2023, the average ransomware payment **increased by 89%** year over year to $1.5 million.[6]

Cryptocurrency investment fraud **rose from $907 million in 2021 to $2.57 billion in 2022,** with the most targeted age group reporting this type of scam being 30-49.[7]

In 2023, it took an **average of 287 days** to identify a data breach. The average time to contain a breach was **80 days.**[8]

As of 2021, the average financial services employee has access to **11 million** files.[9]

Multi-factor authentication blocks **99.9%** of modern automated cyberattacks, **96%** of bulk phishing attempts, and **76%** of targeted attacks.[10]

64% of all businesses have **already experienced** web-based attacks.[11]

The Importance of Proactive Prevention

Proactive prevention is the best defense against cyber attacks. Many of these threats can be prevented with simple security measures. By taking the time to implement these best practices, you can protect yourself and others and help keep your data safe from malicious actors looking to exploit it.

- Update your software
- Use and maintain antivirus software
- Use strong passwords or paraphrases
- Implement multi-factor authentication
- Avoid public Wi-Fi
- Secure your mobile device
- Backup data
- Use caution with email attachments and untrusted links
- Consider using a password manager to generate and store passwords
- Protect your sensitive personal identifiable information (PII)
- Regularly check online accounts and credit reports

In a World of Bad Actors, **#BeTheCyberStar**

[1] Statista – [2] Internet Crime Complaint Center (IC3) – [3] CSO Online – [4] Astra Security – [5] Forbes
[6] SC Media – [7] IC3 – [8] IBM – [9] Varonis – [10] Zippa – [11] Ponemon Insitute

Download the PDF

Dictionary

Phishing	A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.
Ransomware	A type of malicious attack where attackers encrypt an organization's data and demand payment to restore access.
Multi-factor authentication	A system for confirming the identity of a user, process, or device that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors (**e.g., something you know, something you have, and something you are**).

ECStech.com