Cyber Security Awareness Training

Why Should You Care About Cybersecurity?

Real World Hacking Examples

All the below mentioned examples are happening – every day. These examples are selected because they are not so obvious, like stealing credit card information, or did not make the headlines, like political hacks.

Hacking a law firm to learn more about mergers & acquisitions and benefitting through insider trading.

Stealing large quantities of sensitive data from hospitals and other organizations in the health care industry. Medical identity theft allows one to buy drugs that can then be resold.

Disrupting critical infrastructure sectors, including energy, nuclear power, commercial facilities, water treatment, aviation and manufacturing.

Using vulnerabilities to test a system to see if it could be penetrated and then using it for future attacks.

Putting a web server temporarily out of service. Someone can buy a so-called DDos attack for $150 to take your website down for a week.

Customer Protection

When we talk about cyber risk, what's most often at risk is the personal information of customers.

Financial Cost

There are so many factors which impact the financial costs of being hacked, such as paying a ransom to get data decrypted, falling stock prices, investigative and forensic efforts, identity protection services for affected customers, and legal consulting and fees.

Product Protection

Another major target of cyber attacks is a company's intellectual property, such as plans, code, or strategy, and includes communications, such as email, voice mail and shared documents.

Company Reputation

If people associate your brand name with a data breach incident, it's unlikely that they would choose to use your services or product at a later point in time, regardless of what measures you've taken since then.

Career Damage

Lawsuits brought by shareholders against the private individuals running a company are not only possible, but commonplace in the wake of a major breach