CYBER SECURITY
BY SAM MUNAKL

WHAT IS CYBERSECURITY?

Technologies and Processes designed to protect computer networks and data from threat.

UNAUTHORIZED ACCESS	VULNERABILITIES	INTERNET ATTACKS

Cybersecurity standards enable organizations to practice safe security techniques to minimize the number of successful cybersecurity attacks.

WHAT IS THE THREAT?

CYBER HACKERS

- Sophisticated Criminals & Criminal Organizations
- State Sponsored & Governmental Espionage
- Property Thieves
- Someone who has taken a personal interest in you

HACKER TECHNIQUES

- Exploit human behavior
- Exploit system vulnerability
- Physical theft of portable devices
- Email from an infected device

WHAT DO HACKERS WANT?

Financial Gain From Using Or Selling Your Data & Property

- Credit Card Information
- Social Security Number
- Bank Account Information
- Identity Theft

Personal & Third-party Attacks

- Social Accounts
- Email Accounts
- Contact Lists

Industrial or Government Espionage

- Office Financials
- Contact Lists
- Cloud Storage Accounts

WHO IS AT RISK?

Any business, large or small, who is reliant on the internet for daily operations.

Cyber criminals look for weak spots to attack, no matter how large or small the organization. Small businesses, for instance, are becoming a more attractive target as many larger companies tighten their cybersecurity.

WHAT TO DO IF YOU'VE BEEN HACKED?

1. **DON'T PANIC**
2. Contact your IT department
3. Take offline or isolate any servers, machines and parts of the system that house important information.
4. Change your credentials for important online accounts and servers where data is stored.
5. Start adding up what exactly has been lost.
6. Ask yourself pivotal questions such as
   What did the hacker manage to take from me?
   Is that information vital for my company's future?
7. Get with your IT team to find out how the breach occurred. Suspect the human element.
8. Always ask yourself,
   Are your employees happy?
   And what type of access do they have?

HOW CAN YOU PROTECT YOURSELF?

1. Strengthen passwords
2. Install Anti-Virus software
3. Screen suspicious emails
4. Avoid suspicious links

HOW CAN WE HELP?

CYBER SECURITY SERVICES

- Risk Assessment
- Vulnerability Scanning & Penetration Testing
- Enterprise Encryption Solution

- Network & System Security Monitoring
- Computing, Network & Data Policy Compliance

Begin implementing cyber-safety procedures today to protect your company, clients, and employees from the invisible but costly threat of cyber attacks.

CONTACT CYTEK FOR MORE INFORMATION

844.644.8744 | info@cytek.com | www.Cytek.com