Cyber Security

City of Camas
2022

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization.

What is Cybercrime?

► Cybercrime can be defined as "The illegal usage of any communication device to commit or facilitate in committing any illegal act".

► A cybercrime is explained as a type of crime that targets or uses a computer or a group of computers under one network for the purpose of harm.

► Cybercrimes are committed using computers and computer networks. They can be targeting individuals, business groups, or even governments.

What is Cyber Security?

Common Types of Cyber Attacks

▶DDoS attacks

▶Ransomware

▶Identity Theft

▶Social Engineering

▶Phishing

▶Exploit kits/Ransomware

▶PUPs and Malware

What is the IMPACT?

Impact of attacks in the US

▶ **"State Sponsored Threats:** According to Microsoft, nearly 80% of nation-state attackers targeted government agencies.

▶ **Phishing Attacks:** Phishing attacks were connected to 36% of breaches, an increase of 11%, which in part could be attributed to the COVID-19 pandemic. Threat actors have been observed tweaking their phishing campaigns based on what's making the news at any moment in time. (Verizon 2021 Data Breach Investigations Report)

▶ **Cost of Data Breach:** 2021 saw the highest average cost of a data breach in 17 years, with the cost rising from US$3.86 million to US$4.24 million on an annual basis. (IBM Cost of a Data Breach Report 2021)

▶ **Ransomware Payouts:** Cryptocurrency has been the preferred payment method for cybercriminals for a while now, especially when it comes to ransomware. As much as US$5.2 billion worth of outgoing Bitcoin transactions may be tied to ransomware payouts involving the top 10 most common ransomware variants. (FinCEN Report on Ransomware Trends in Bank Secrecy Act Data)

▶ **DDoS Attacks:** The number of distributed denial-of-service (DDoS) attacks has also been on the upward trend, in part due to the COVID-19 pandemic. 2020 saw more than 10 million attacks occur, 1.6 million attacks more than the previous year. (ENISA Threat Landscape 2021)

Most Targeted Sectors Worldwide by Hackers in 2021

- ▶ Education/Research sector up by 75%
- ▶ Cyber attacks on Healthcare sector up by 71%
- ▶ ISP/MSP up by 67%
- ▶ Communications +51%
- ▶ Government / Military sector up by 47%

Cyber attacks on small to medium sized businesses, are becoming more frequent, targeted, and complex. According to Accenture's Cost of Cybercrime Study, 43% of cyber attacks are aimed at small organizations, but only 14% are prepared to defend themselves.

According to Ponemon Institute's State of Cybersecurity Report, small to medium sized business around the globe report recent experiences with cyber attacks:

- **Insufficient security measures**: 45% say that their processes are ineffective at mitigating attacks.

- **Frequency of attacks**: 66% have experienced a cyber attack in the past 12 months.

- **Background of attacks**: 69% say that cyber attacks are becoming more targeted.

The most common types of attacks on small businesses include:

- **Phishing/Social Engineering**: 57%

- **Compromised/Stolen Devices**: 33%

- **Credential Theft**: 30%

Cyber Security….. Why it's happening now

Threat evolution

- ▶ Increasing sophistication of attackers
- ▶ Commoditization of exploitation
- ▶ "Lower barrier to entry" for attacker

Risk and Reward

- ▶ Low risk (detection, capture, penalty)
- ▶ Potential significant reward for success
- ▶ New motivations

It is a Hot Topic

- ▶ Intense and prolific media coverage
- ▶ High exposure for affected organizations

Hackers demands $200k ransom from Tri-Cities port to unlock computer data, Port of Kennewick, Benton County

City of Lacey, Thurston County

Breach Type – Hacking, Data Breach

K5 News

November 7th, 2019
- Credit card information stolen by ba[...] hacked "Click2Gov" services
- Information was stolen after custom[...] online
- Officials believed customers that sig[...] auto-pay likely had information stole[...]

said the personal information of p[...]
millions of licensed professionals [...]
exposed after it detected suspicio[...]
its online licensing system."

Town of Tenino defrauded out of almost $300,000, Thurston County

Breach Type – Phishing, Other

gton

Big Country News Connection

January 15th, 2022
- "The Office of the Washington State Auditor has released its findings on how the town of Tenino was bilked out of nearly $300,000 in 2020."
- "According to the report, the person who was serving as the city's clerk-treasurer at the time was scammed into sending the money out of state by a phishing email."

Compliancy Group

September 8th, 2021
- "Hacking incidents have continually been the prime reason behind the escalating breaches targeting healthcare organizations."
- "There were 26 healthcare providers targeted by hacking incidents in July, affecting 3,200,815 patients, representing 69.63% patients affected by hacking."

City of Puyallup, Pierce County

Breach Type – Unknown, Data Breach

The Suburban Times

February 18th, 2021
- Third party vendor AFTS was victim of ransomware cyberattack
- City officials believed no direct threat to the city was evident
- Compromised data potentially included account numbers, names, addresses, and bill amounts

Cyber crimes can happen to any organization, including those in our backyard!

What is the City of Camas doing to protect our data?

What are we doing now…

- Continued cyber security training
- Infrastructure security
- Endpoint Security
- Firewalls & VPN
- Multi factor authorization (MFA - in progress)

What's to come…

- Updating organization-wide software
- Leveraging group partnerships for technology purchases
- Continued investment in network infrastructure
- Implementing a more rigorous testing regimen
- Updates to policies and procedures