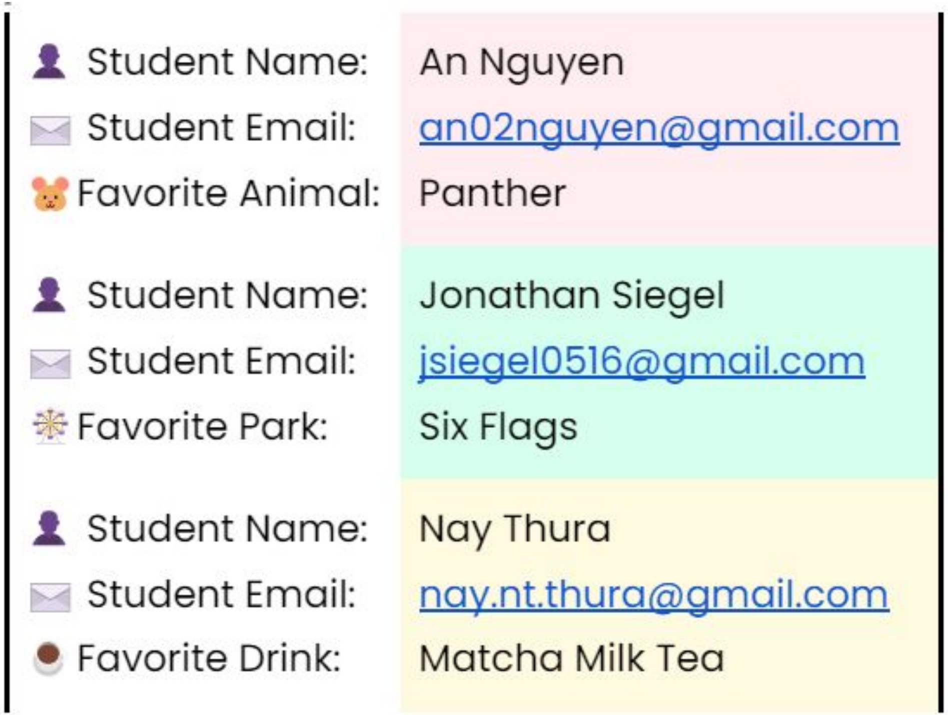
Group 52:



Student Name:	An Nguyen
Student Email:	an02nguyen@gmail.com
Favorite Animal:	Panther
Student Name:	Jonathan Siegel
Student Email:	jsiegel0516@gmail.com
Favorite Park:	Six Flags
Student Name:	Nay Thura
Student Email:	nay.nt.thura@gmail.com
Favorite Drink:	Matcha Milk Tea

CODEPATH*ORG

Malware

To: PHI$H TANK

By: An Nguyen, Jonathan Siegel, Nay Thura

Agenda

1	Intro	00:00 - 00:30
2	What is Malware?	00:30 - 01:30
3	Risk / Mitigation #1	01:30 - 02:30
4	Risk / Mitigation #2	02:30 - 03:30
5	Risk / Mitigation #3	03:30 - 04:30
6	Conclusion / Wrap-Up	4:30 - 5:00

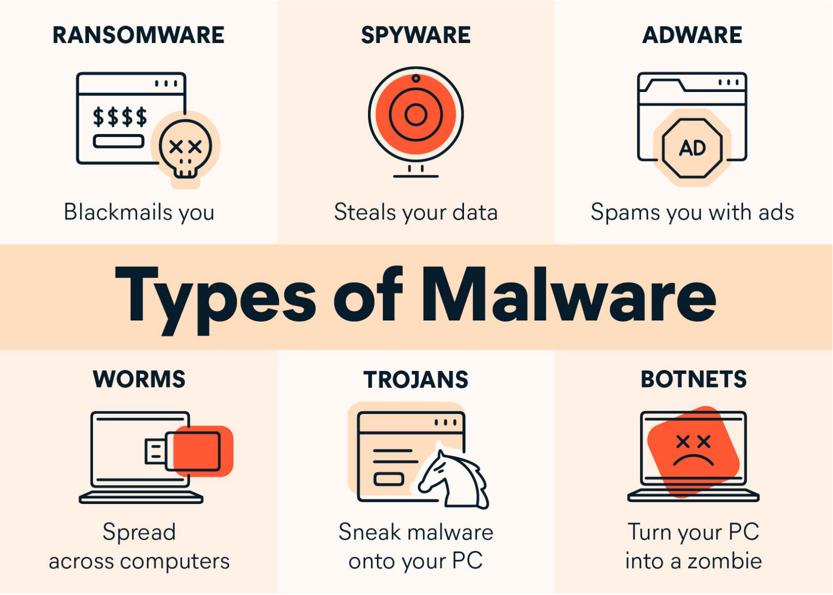
What is Malware?

- Malware: short for "malicious software"
  - Any program or code designed to harm or disrupt computer systems, networks, or devices
- Forms:
  - Viruses, worms, Trojans, ransomware, adware, and spyware
- Malware can infect a computer system in a variety of ways:
  - Email attachments, malicious websites, or software downloads from untrusted sources
- Once a system is infected, malware can perform a wide range of malicious activities:
  - Stealing sensitive data, disrupting network traffic, encrypting files, or even taking control of the entire system.

Why Should Malware be a concern?

Damages from Malware

- Identity theft
- Financial loss
- Personal data breaches
- Personal information leaks



Types of Malware

RANSOMWARE
Blackmails you

SPYWARE
Steals your data

ADWARE
Spams you with ads

WORMS
Spread across computers

TROJANS
Sneak malware onto your PC

BOTNETS
Turn your PC into a zombie

Steps for Protection from Malware

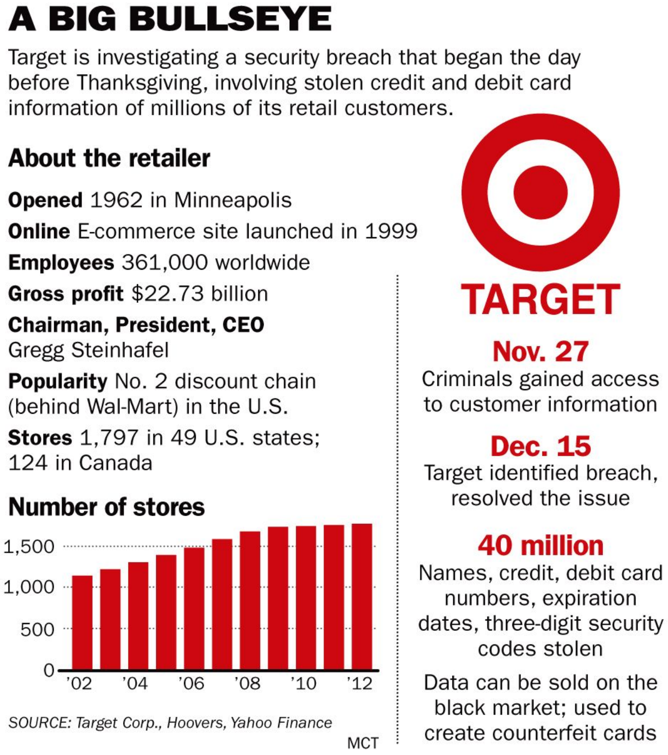
- Install reliable antivirus program.
- Educate yourself about malware for prevention steps.
- Create a data backup plan.
- Keep systems up to date.
- Beware of providing sensitive information.

AVG
ULTIMATE
SECURITY, PRIVACY, & PERFORMANCE
Antivirus & anti-ransomware
Shopping & banking protection
Firewall & webcam security
All-in-one cleanup & tuneup
VPN for private browsing
Auto software updater
10 DEVICES
2 YEARS
CONTINUOUS PROTECTION
Renews automatically each year
1 year pre-paid subscription
norton
1 DEVICE
Norton
AntiVirus Plus
Powerful protection for your connected world
100% GUARANTEE
PC EDITORS' CHOICE
Malwarebytes
PREMIUM
5 Devices 1 Year Subscription
omprehensive Cybersecurity for PC, Mac, and Android
"The Best Antivirus Is Not Traditional Antivirus."
— Wirecutter (A New York Times Company)

Risk #1: Target Data Breach

- In 2013, hackers attacked and stole data from Target
- Stolen credit and debit card information from 40 million Target customers
- Stolen personal information from 70 million customers, in one of the largest data breaches in history.

- Risk: Customers and their personal information, including money, addresses, contact info, etc…



A BIG BULLSEYE

Target is investigating a security breach that began the day before Thanksgiving, involving stolen credit and debit card information of millions of its retail customers.

About the retailer

Opened 1962 in Minneapolis

Online E-commerce site launched in 1999

Employees 361,000 worldwide

Gross profit $22.73 billion

Chairman, President, CEO
Gregg Steinhafel

Popularity No. 2 discount chain (behind Wal-Mart) in the U.S.

Stores 1,797 in 49 U.S. states; 124 in Canada

Number of stores

SOURCE: Target Corp., Hoovers, Yahoo Finance

MCT

Nov. 27
Criminals gained access to customer information

Dec. 15
Target identified breach, resolved the issue

40 million
Names, credit, debit card numbers, expiration dates, three-digit security codes stolen

Data can be sold on the black market; used to create counterfeit cards

Mitigation Strategies #1

- Organizations should implement strong security measures:
  - Access controls
  - Firewalls
  - Intrusion detection
  - Prevention systems
- Organizations should regularly monitor their systems
  - Suspicious activity
  - Conduct regular security audits
  - Provide security awareness training to employees.

Risk #2: Hospital Ransomware in Paris

- Hospital in Paris was under attack from ransomware.
- All computer systems were shut down.
- Attacker demanded $10,000,000.

- What were at risk?
  - The patients at the hospital were at risk.
  - The hospital was facing a financial threat.

- Why should businesses be worried about this?

Mitigation Strategies #2

- Hospital isolated themselves from infected hardware.
- What else could the hospital have done?
  - Install a reliable antivirus software.
  - Educated employees to be aware of suspicious emails or files they download.
  - Create backup data plan to protect and preserve data in case of an attack.

Risk #3: NotPetya Malware Attack

- In June 2017, the NotPetya malware attacked organizations worldwide, causing billions of dollars in damage
- NotPetya used stolen NSA hacking tools and spread through a software update from a Ukrainian accounting software company

- Risks: organizations, companies - their money, trust factors from customers, etc…

NotPetya: A New Breed of Malware
As malware attacks like NotPetya grow more and more sophisticated, how can you ensure your business and your data are safe?

Mitigation Strategies #3

- To mitigate the risk of NotPetya and similar attacks, organizations should:
  - Follow best practices for supply chain security, such as verifying the security of third-party software vendors and their products.
  - Segment their networks to prevent the spread of malware, implement strong access controls, and have a robust incident response plan in place.

Conclusion/Wrap up

- Malware poses significant risks to individuals and organizations alike
  - Including data theft, system disruption, and ransomware attacks

- Implementing effective mitigation strategies → organizations can reduce their risk of malware infections and protect themselves from the potentially devastating consequences of cyberattacks

- Some key mitigation strategies include:
  - Keeping software up to date and patching vulnerabilities
  - Using antivirus software and regularly scanning systems for malware
  - Educating users on safe browsing habits and providing regular security awareness training
  - Regularly monitoring systems for suspicious activity