

# Personal Cybersecurity

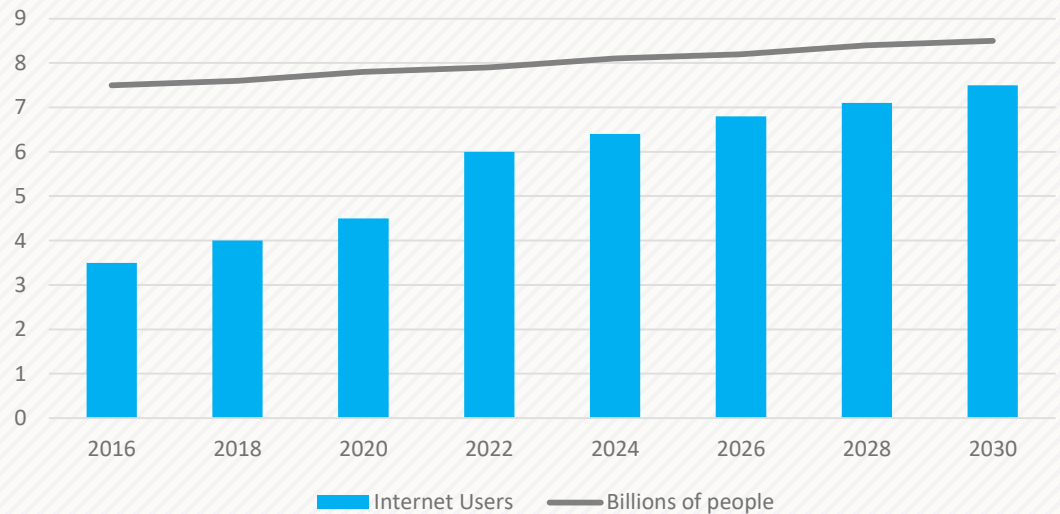
The Basic Principles

**Jeremiah School, CEO**

# How big is the issue?

**\$4.5**  
**TRILLION**

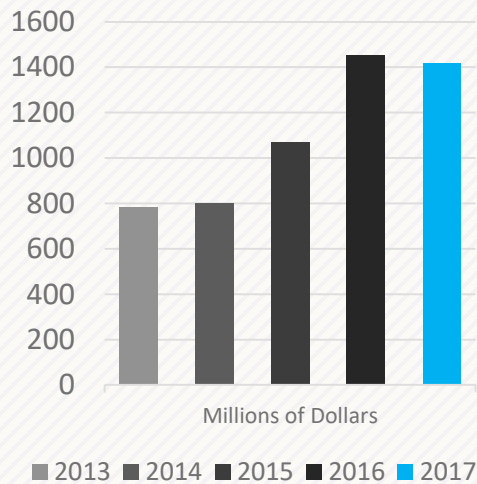
Estimated global  
damages in 2018



Internet users vs world population trend

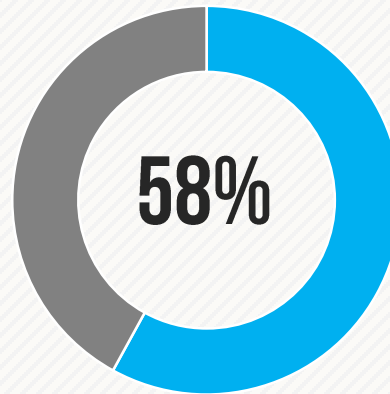
Source: *Cybersecurity Ventures 2018*

# How big is the issue?



Reported cybercrime losses by Americans

Source: FBI IC3 2017



Americans are victims of cybercrime

Source: Symantec 2017



Reported cybercrime losses by Wisconsinites

Source: FBI IC3 2017

**What are they looking for?**

**What do they want to do?**

**How do they get my data?**

**How do I protect myself?**

**What if I become a victim?**

# What are they looking for?

Personal Information

Passwords

Email Accounts

# What are they looking for?

## Personal Information

- Social Security information
- Drivers license numbers
- Credit card numbers
- Account information
- Trading information
- Social information for building a convincing persona
- Intellectual property
- Anything that can be used for ransom

Passwords

Email Accounts

# What are they looking for?

Personal Information

Passwords

- Gain access to higher valued assets
- Gain access to bank accounts
- Gather payment card details
- Make fraudulent purchases

Email Accounts

# What are they looking for?

Personal Information

Passwords

Email Accounts

- Password reset requests
- Tax, travel, and order information
- Spamming contacts
- Leverage social engineering opportunities



# What do they want to do?

Extort Money

Utilize Your Resources

Disrupt & Destroy

# What do they want to do?

Extort Money

Ransomware

- Encrypting your files until a ransom is paid
- Encrypts all files available
- Between \$400 and \$1400, more for businesses
- Mobile ransomware is growing quickly

Identity Theft

Scare Tactics & Blackmail

Utilize Your Resources

Disrupt & Destroy

# What do they want to do?

Extort Money

Ransomware

Identity Theft

- Tax fraud
- Setup credit cards
- Open up lines of credit
- Falsify employment records
- Obtain medical care
- Insurance fraud

Scare Tactics & Blackmail

Utilize Your Resources

Disrupt & Destroy

# What do they want to do?

Extort Money

Ransomware

Identity Theft

Scare Tactics & Blackmail

- False scares of having a virus
- Warnings of device being locked
- Threats of personal harm
- Use of cameras and photos for blackmail

Utilize Your Resources

Disrupt & Destroy

# What do they want to do?

Extort Money

Ransomware

Identity Theft

Scare Tactics & Blackmail

Utilize Your Resources

- Turning your device into a bot
- Used for spamming, crypto mining and denial of service attacks
- Used for brute force attacks and password cracking
- Used in social media for mass info dumping and creating trends

Disrupt & Destroy

# What do they want to do?

Extort Money

Ransomware

Identity Theft

Scare Tactics & Blackmail

Utilize Your Resources

Disrupt & Destroy

- Hacktivism & political purposes
- Personal sabotage or popularity
- Damage equipment
- Distraction for larger & more complex attacks

# How do they get my data?

Phishing

Spoofing

Password Cracking

# How do they get my data?

## Phishing

### **Email Phishing**

Legitimate-looking emails that appear as though they originated from reputable sources often including links, documents and pictures

### **Phone / Voice Phishing**

Is a form of criminal phone fraud, using social engineering over the telephone system to gain access to private personal and financial information

## Spoofing

Email

Websites

Phone / Caller ID

## Password Cracking



# How do they get my data?

Phishing

Spoofing

Email

- Requests for help and money from contacts
- Baiting with great deals
- Fraudulent bank wire fund transfers

Websites

Phone / Caller ID

Password Cracking

# How do they get my data?

Phishing

Spoofing

Email

Websites

- Banking websites
- Government agency
- Those asking for personal information

Phone / Caller ID

Password Cracking

# How do they get my data?

Phishing

Spoofing

Email

Websites

Phone / Caller ID

- Microsoft calling to inform you of a virus
- Workplace IT Support
- Government agency
- Winning a prize

Password Cracking

# How do they get my data?

Phishing

Spoofing

Email

Websites

Phone / Caller ID

Password Cracking

- Brute Force
- Social Engineering
- Snooping

# How do I protect myself?

# How do I protect myself?

## Updating & Upgrading

Firewalls

Smart Devices

Antivirus & Antimalware

Wireless Connections

Email

Phone

Passwords

Backups

Credit & Debit Cards

Identify Theft Protection

Cyber Security Insurance

Protecting Children

Other

- Update vs Upgrade
- Be aware of *end of support* dates
- Ensure hardware and software stays up to date
- Utilize automatic update settings where possible

# How do I protect myself?

Updating & Upgrading

Firewalls

Smart Devices

Antivirus & Antimalware

Wireless Connections

Email

Phone

Passwords

Backups

Credit & Debit Cards

Identify Theft Protection

Cyber Security Insurance

Protecting Children

Other

- Ensure you have a hardware and software firewall
- Ensure software is up to date
- Maintain opened and forwarded ports if used
- Disable remote access

# How do I protect myself?

Updating & Upgrading

Firewalls

Smart Devices

Antivirus & Antimalware

Wireless Connections

Email

Phone

Passwords

Backups

Credit & Debit Cards

Identify Theft Protection

Cyber Security Insurance

Protecting Children

Other

- Take inventory
- Use strong passwords on all devices
- Disable remote access to the device unless necessary
- Keep them up to date



# How do I protect myself?

Updating & Upgrading

Firewalls

Smart Devices

Antivirus & Antimalware

Wireless Connections

Email

Phone

Passwords

Backups

Credit & Debit Cards

Identify Theft Protection

Cyber Security Insurance

Protecting Children

Other

- Have antivirus software installed
- Ensure it's up to date
- Setup to run prescheduled scans
- All operating systems are vulnerable

# How do I protect myself?

Updating & Upgrading

Firewalls

Smart Devices

Antivirus & Antimalware

Wireless Connections

Email

Phone

Passwords

Backups

Credit & Debit Cards

Identify Theft Protection

Cyber Security Insurance

Protecting Children

Other

- Use public Wi-Fi cautiously
- Secure your home wireless network
- Do not auto connect to wireless networks
- Remove unused Wi-Fi networks and Bluetooth devices

# How do I protect myself?

Updating & Upgrading

Firewalls

Smart Devices

Antivirus & Antimalware

Wireless Connections

Email

Phone

Passwords

Backups

Credit & Debit Cards

Identify Theft Protection

Cyber Security Insurance

Protecting Children

Other

- Be aware of what's in your inbox and sent items
- Be on the look out for email spoofing and phishing
  - Examine & verify the senders email address
  - Examine & verify link URL's
- Verify suspicious email by calling person or company
- Do not send personal or sensitive information

# How do I protect myself?

Updating & Upgrading

Firewalls

Smart Devices

Antivirus & Antimalware

Wireless Connections

Email

Phone

Passwords

Backups

Credit & Debit Cards

Identify Theft Protection

Cyber Security Insurance

Protecting Children

Other

- Don't answer questions or push buttons
- Hang up and call person or company
- Setup voicemail passwords or change default

# How do I protect myself?

Updating & Upgrading

Firewalls

Smart Devices

Antivirus & Antimalware

Wireless Connections

Email

Phone

Passwords

Backups

Credit & Debit Cards

Identify Theft Protection

Cyber Security Insurance

Protecting Children

Other

- Use 2 Factor Authentication
- Do not reuse passwords
- Do not use a variation of your previous passwords
- Use long passwords, over 12 characters
- Use long memorable phrases
- Change password(s) at any concern of being hacked
- Assess how critical the account is
- Utilize password managers

# How do I protect myself?

Updating & Upgrading

Firewalls

Smart Devices

Antivirus & Antimalware

Wireless Connections

Email

Phone

Passwords

Backups

Credit & Debit Cards

Identify Theft Protection

Cyber Security Insurance

Protecting Children

Other

- If possible leverage cloud backup products
- Automate the process
- Verify and monitor
- Test restore

# How do I protect myself?

Updating & Upgrading

Firewalls

Smart Devices

Antivirus & Antimalware

Wireless Connections

Email

Phone

Passwords

Backups

Credit & Debit Cards

Identify Theft Protection

Cyber Security Insurance

Protecting Children

Other

- Review accounts
- Freeze your credit
- Use credit cards for online purchases
- Avoid storing card information on sites
- Be aware of payment card overlays

# How do I protect myself?

Updating & Upgrading

Firewalls

Smart Devices

Antivirus & Antimalware

Wireless Connections

Email

Phone

Passwords

Backups

Credit & Debit Cards

Identify Theft Protection

Cyber Security Insurance

Protecting Children

Other

- Secure personal information
- Freeze your credit with all credit rating agencies
- Follow other technology best practices
- Evaluate identity protection services



# How do I protect myself?

Updating & Upgrading

Firewalls

Smart Devices

Antivirus & Antimalware

Wireless Connections

Email

Phone

Passwords

Backups

Credit & Debit Cards

Identify Theft Protection

Cyber Security Insurance

Protecting Children

Other

- Coming to the consumer market
- Assisting with losses such as IoT devices, ransomware, and identity theft
- Understand the details

# How do I protect myself?

Updating & Upgrading

Firewalls

Smart Devices

Antivirus & Antimalware

Wireless Connections

Email

Phone

Passwords

Backups

Credit & Debit Cards

Identify Theft Protection

Cyber Security Insurance

Protecting Children

Other

- Use parental control software
- Use privacy settings on social media sites
- Bring awareness to cyber risks
- Setup and freeze credit

# How do I protect myself?

Updating & Upgrading

Firewalls

Smart Devices

Antivirus & Antimalware

Wireless Connections

Email

Phone

Passwords

Backups

Credit & Debit Cards

Identify Theft Protection

Cyber Security Insurance

Protecting Children

Other

- Annual audits
- Change from Administrative to User account
- Isolate activities to devices you manage and trust
- Remove unneeded and unused software "bloatware"
- Avoid 3rd party software add-ons during installs

# What if I become a victim?

Take immediate action

Notify needed parties

Report the crime

# What's Next?

Global, National, and Local Authority

Better software development

No more passwords

Quantum computing

# Questions?

# Thank you!

**Jeremiah School**

920-321-3622

[jschool@weareinnova.com](mailto:jschool@weareinnova.com)