# PERSONAL CYBERSECURITY 101

**Be smart. Stay safe online and protect your digital footprint.**

Presented by

ACUMEN
SOLUTIONS GROUP

# Why Would Someone Hack You?

You see the headlines all the time, but hackers don't just go after the big fish. They'll target anyone who's easy prey.

The list of cyber risks individuals face is growing all the time.

Protecting yourself from these threats is key.

Learn how to detect and prevent cyber-attacks and bring cybersecurity into your home.

# Inside This E-book

Welcome to the Wild, Wild Web ..... 5

Chapter 1: A Look at Major Cyber Dangers ..... 6

Chapter 2: Main Causes of Security Breaches ..... 13

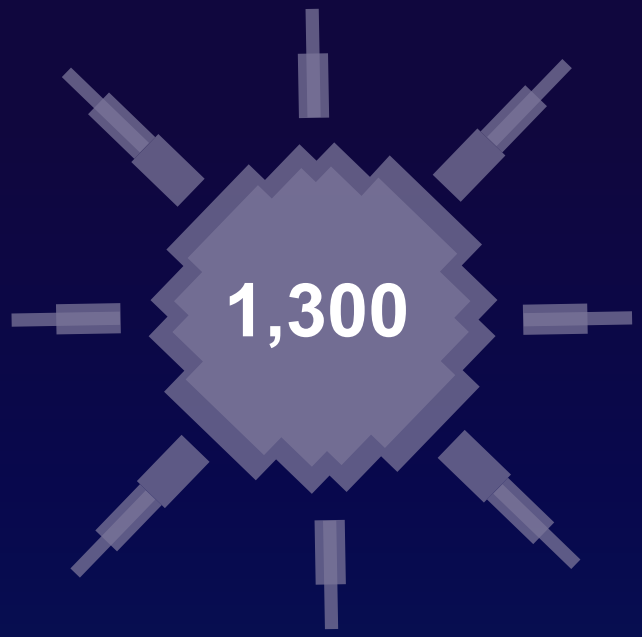
Chapter 3: Personal Cyber Insurance ..... 18

Chapter 4: Best Practices To Avoid Threats ..... 21

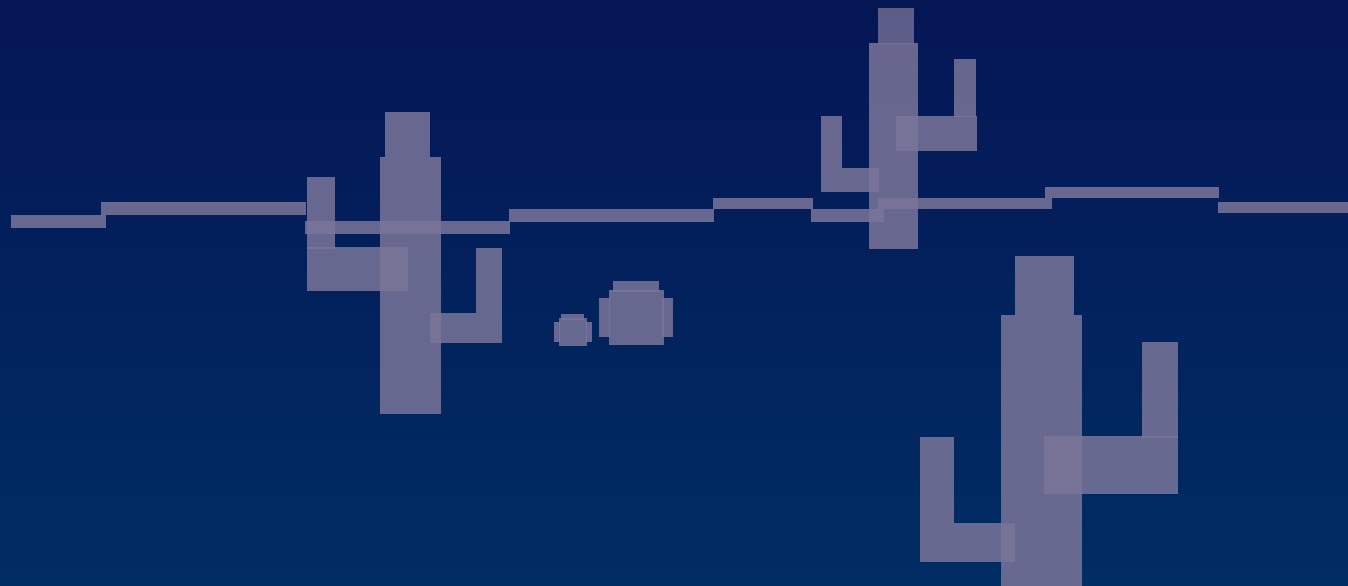
# Welcome to the Wild, Wild Web

It's easy to dismiss cyberattacks as something that happens to big companies—or other people—but the threat is real, and growing. If you don't take steps to protect yourself, you could become the next victim.

We'll look at some of the many cyber risks out there, and how to avoid falling prey to scams and ID theft.




**Average number of reported cybercrime complaints per day[1]**



## Chapter 1

# A Look at Major Cyber Dangers

# Targeting Your Money and Good Name

If your banking information is compromised or stolen, it can be the start of a series of problems that go far beyond theft. In addition to possibly draining your accounts, crooks may use your personal information to open new accounts or take out loans in your name.

While fraudsters disappear with your hard-earned money after cloning your identity, you'll be left with the fallout. Frequently, this will involve payment default notices and a damaged credit report, which may only become known several months after the fraud was perpetrated.

Life will likely get very complicated and expensive. And this is only one example of cyber dangers.

# 10 Common Cyber Threats

## 1. Malware

Software that performs a malicious task on a target device or network, such as corrupting data or taking over a system.

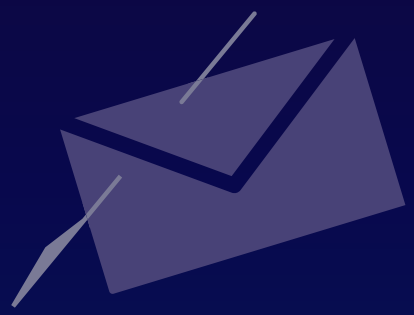
**Example:** You accidentally download malware that's disguised as free security software.

## 2. Phishing

An email-based scam that encourages recipients to click on a legitimate-looking link and disclose confidential info or inadvertently download malware.

**Example:** You receive an email from your bank asking you to access your account to confirm recent privacy changes. The email and website both seem legitimate, but careful investigation is needed.

# 10 Common Cyber Threats



## 3. Spear Phishing

A more targeted form of phishing that uses specific information about the intended victim to gain trust and encourage action.

**Example:** You get an email that appears to be from ABC Bank—which is your bank—asking you to click a link and confirm your account information.

## 4. Data Breaches

A data breach is theft of data by a hacker. Motives for attacks may include crime (i.e., identity theft), a desire to embarrass an institution (e.g., Edward Snowden or the DNC hack) or espionage.

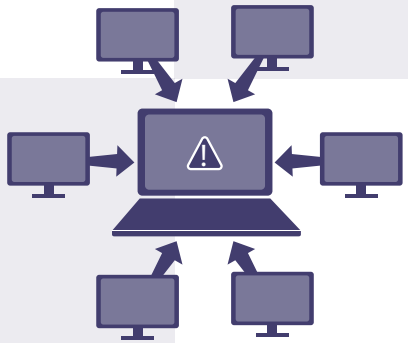
**Example:** Corporations are prime targets for hackers attempting to steal large amounts of valuable records belonging to millions of customers. Personal and/or financial information, like login credentials and credit card numbers, can be resold on the black market.

# 10 Common Cyber Threats

## 5. Trojans

Named after the Trojan Horse of ancient Greek history, the Trojan is a type of malware that looks harmless, but then lets out malicious code once it has access to your device.

**Example:** You have just accessed an online game for your child that offers a free download. This download is in fact malware.



## 6. Distributed Denial of Service Attack (DDoS)

Where an attacker takes over thousands of devices and uses them to target a server, causing the website to crash from an overload of demand.

**Example:** If your computer is infected with malware, it could be used in a DDoS attack.

# 10 Common Cyber Threats

## 7. 'Man in the Middle'

Where an attacker intercepts electronic messages, perhaps changing them in transit. The sender and recipient believe they are communicating directly with one another.

**Example:** A cybercriminal sets up a Wi-Fi connection with a legitimate-sounding name, similar to a nearby business. Once you connect to the fraudster's Wi-Fi, the attacker may intercept passwords, payment information and more.

## 8. Ransomware

Attack that involves encrypting data and demanding a ransom in exchange for letting you have access to your online documents again.

**Example:** These attacks range from low-level nuisances to serious incidents like locking down municipal government data or hospital records.

# 10 Common Cyber Threats

## 9. Mobile Devices

Mobile devices are vulnerable to malware attacks just like any other hardware. Attackers may embed malware in apps, websites, emails or text messages. Once compromised, your device can give the cybercriminals access to personal information, location data, financial accounts and more.

**Example:** If you use your phone for two-factor identification, you may feel safe when your bank sends you a text with a verification code when you're logging in. But if hackers have taken control of your phone number, they can see that code—and, ultimately, access your account info.

## 10. Smart Devices

Given their numbers, smart devices are a prime target for criminals. Devices like your activity tracker, smartwatch or smart TV are vulnerable to multiple types of cyber threats including hackers taking over the device to make it part of a DDoS attack or to gain unauthorized access to data being collected by the device.

**Example:** A hacker can remotely access a child's smartwatch GPS tracker and alter its geographic location, leading parents to believe their child is in an inaccurate location. Similarly, by accessing the smartwatch's SIM card, a hacker can listen to what the user is saying.

## Chapter 2

# Main Causes of Security Breaches

# How Does Your Data Become Vulnerable?

Data leaks happen. As long as personal information is available online, it's vulnerable to an accidental or intentional disclosure.

Most cyber breaches are the direct result of compromised or stolen credentials. Let's take a closer look at how you can become a victim.

## Human Error

The major causes of individual security breaches — hacking, phishing and malware — are often the result of human error.

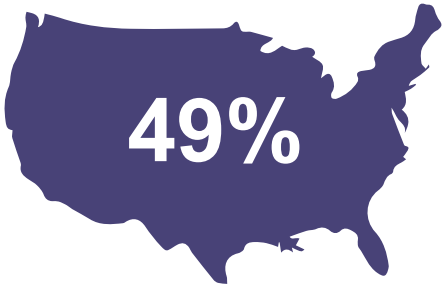
The good news is, with proper training, you and your family can become masters at preventing cyberattacks. Awareness and education are critical in the fight against security breaches.

## Hacking

Although antivirus software and firewalls will protect you in many instances, a hacker may maliciously target you and gain access to your computer network or devices, corrupt data or steal files.

Do you own any smart, internet-connected home devices? The chances of your smart doorbell or fridge being targeted by hackers are relatively slim. But your home security system or smart TV may be a vulnerable and desirable target.

The more commonplace devices like these become, the greater the inherent risk. Partly, this can be due to a lack of awareness and understanding of what smart devices are and how they function.




**U.S. data breaches caused by human error**[2]

**Increase in attacks by mobile banking malware in the first half of 2019**[3]

## Identity Theft

Identity theft occurs when someone else obtains and uses your personal data or documents, without permission, to obtain money, goods or services. Falling victim to identity theft can be emotionally and financially devastating.

## Cyber Extortion

Cyber extortion most commonly occurs in the form of ransomware, which is often spread through emails pretending to be from reputable sources or someone you know. Once opened, malware may disrupt or lock your device, threaten to encrypt or delete data, or threaten to share your device information unless a ransom is paid.

Malware is often sophisticated and may require payment to free your device or decrypt your data. You may also need the advice and support of an expert to help you.

**U.S. adults who have experienced identity theft - more than twice the global average[4]**

**Malware delivered via email[5]**

## Online Shopping

Although online shopping is convenient, it's also a common target for criminals. Always order from reputable online stores that have a history of excellent customer satisfaction. Major retailer sites and Amazon are, for the most part, a safe bet.

Any site you buy from should have 'https' in the address bar or a padlock icon to show that it's secure. Some browsers highlight unsecured web addresses in red. You can also consult Google's safe site search, and check customer comments and reviews before you make a purchase.

Avoid making purchases over public Wi-Fi. Bad actors can intercept your connection and access your information. If you must use public Wi-Fi, connect to a virtual private network (VPN).

## Cyberbullying

Online harassment or intimidation can be serious. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else.

Defamation of character, invasion of privacy or threats of violence committed against you online can lead to psychological stress, unexpected legal expenses, and even parent liability for claims brought against you due to a child's cyberbullying activities.

**80.5% of consumers reporting online purchase scams in 2020 lost money[6]**

**Share of adult internet users in the U.S. who reduced their online activity due to digital harassment[7]**

## Chapter 3

# Personal Cyber Insurance

# How Can Insurance Help?

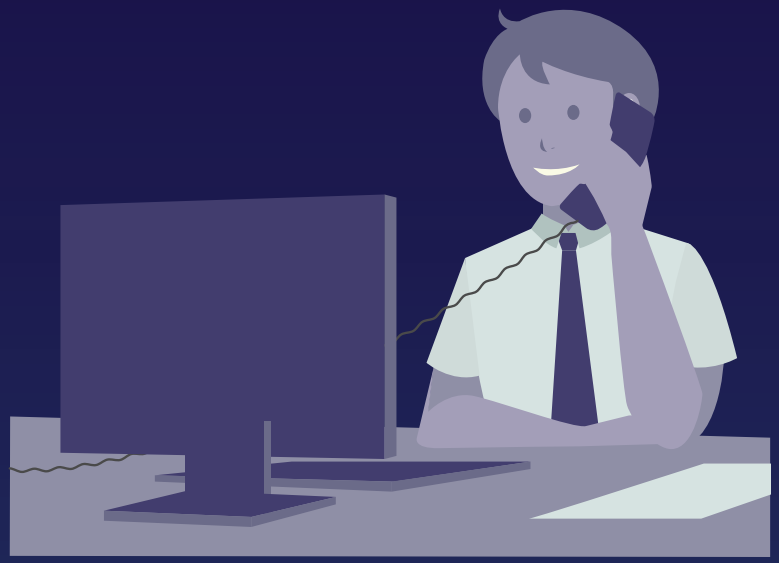
Insurance can't prevent a cyberattack but it can shield you from some of the consequences. Even the most vigilant and online-savvy people face ongoing risks.

Personal cyber protection can often be added to a homeowners, renters or condominium policy. It can also be purchased as a standalone policy.

What if your identity is stolen or a cyberattack makes your house uninhabitable by taking over smart devices? Personal cyber coverage offers protection.

The availability and benefits of personal cyber insurance is evolving as technology proliferates further into our lives and more risks are a threat to our finances and well-being.

Always know what your available personal cyber insurance covers, what your total coverage amount is, and what sorts of situations might negate coverage.



**Ask your insurance professional about what personal cyber insurance is best for your particular situation!**

## Other benefits a policy can provide may include:

- Replacement or repair of damaged devices
- Protection against loss of account funds from a cyberattack and related expenses
- Help with resolving identity theft and the related complications
- Reimbursement of extortion money paid to hackers using ransomware
- Retrieval, replacement or re-creation of lost or destroyed financial, legal or personal identification documents
- Lawsuit protection for allegations of unintentional libel, slander or invasion of privacy
- Credit card protection from fraudulent charges made without your authorization
- Help with dealing with the fallout from online harassment
- Repair to a damaged personal reputation or compromised physical security

Chapter 4

# Best Practices To Avoid Threats

**“Passwords are like underwear: you don’t let people see it, you should change it very often, and you shouldn’t share it with a stranger.”**

— Chris Pirillo, founder and CEO of LockerGnome, Inc.

# Take responsibility for your personal cybersecurity and learn good habits.

# Follow these best practices:

### Use strong passwords

Use unique passwords for every account and create passwords that are difficult to guess. Change your password at least once per year as a safety precaution. If you want an easier way to manage your passwords, try using a password management tool.

### Use two-factor or multi-factor authentication

With two-factor authentication, you're prompted to enter one additional authentication method such as a personal code, another password or even fingerprint. This adds additional layers of security to the standard password method of online identification.

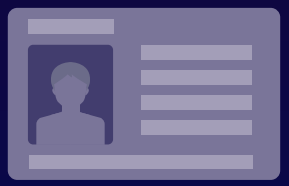
### Keep software up to date

Have security software and run automated software updates. Install anti-virus protection from a trusted vendor to fight malicious attacks. Use a firewall to help screen out hackers, viruses and other malicious activity that occurs over the internet.

### Backup your data regularly

Valuable data like work files and photos should be saved often in a cloud platform and on a hard drive. If you become a victim of ransomware or malware, the only way to restore your data is to erase your systems.

## Protect your sensitive personal identifiable information (PII)



This includes any information that can be used by a cybercriminal to identify or locate you. PII includes:

- Name
- Address
- Phone numbers
- Date of birth
- Social Security Number
- Passport number
- Driver's license number
- Credit card numbers
- Email addresses
- Log in details
- IP address
- Location details

## Secure smart home devices

Ensure home IoT devices have security in place. Read your owner's manual and install security updates as recommended.

## Only shop on secure websites

Bank and shop only on websites with extra security indicated by a 'https' URL.

## Carefully screen emails

Only open email attachments if they come from recognized contacts, and never give out personal information or passwords in response to emails.

If you receive an email with only a link in the message, don't click on the link unless you're expecting the email or verify with the sender the link is legitimate.

## Protect your mobile devices

As mobile devices evolve, they present an increasingly rich and desirable target for cybercriminals. Create a difficult passcode and only install apps from trusted sources. Don't download anything to your device until you are confident about the source.

Frequently update both operating systems and apps so they have the latest security protections. Avoid sending sensitive information over text message or email.

## Review online accounts and credit reports frequently

Safeguard your online accounts and monitor your credit reports. A credit freeze may be the most effective way to protect your personal credit information from cybercriminals.

**Amount recovered by FBI from online scams in 2019**[8]

**Amount lost to cybercriminals in 2019**[9]

# TAKE CONTROL

## Contact us today!

In the coming years, personal cyber insurance might be a necessity given how brazen cybercriminals are becoming.

As your insurance professionals, we're here to discuss coverage options available to you and your family and explore whether now is the time to add personal cyber coverage.

## Sources:

1 - FBI - 2019 Internet Crime Report, February 2020, fbi.gov

2 - IBM - IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years, July 2019, newsroom.ibm.com

3 - ThreatMark - Banking Malware & Attack Vectors Outlook For 2020 (Part 1), June 2020, threatmark.com

4 - IdentityForce - What Are Your Odds of Getting Your Identity Stolen? October 2020, identityforce.com

5 - Forbes - Phishing: Not Just For Criminals, September 2019, forbes.com

6 - Better Business Bureau - BBB research shows spike in online purchase scams since COVID started, October 2020, bbb.org

7 - Statista - Cyber bullying - statistics & facts, October 2020, statista.com

8 - FBI - 2019 Internet Crime Report Released, February 2020, fbi.gov

9 - FBI - 2019 Internet Crime Report Released, February 2020, fbi.gov

**Acumen Solutions Group, LLC**
(516) 986-3425
insurance@acumenins.com

**Acumen Solutions Group, LLC**
600 Broadhollow Road
Suite 200
Melville, NY 11550
acumenins.com/

**CONFIDENTIALITY NOTICE: This email message is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. If you received this electronic transmission in error, please be aware that any unauthorized review; copying, use, disclosure or distribution of this information is prohibited. If you are not the intended recipient, please contact the sender by reply email, then delete the original message, including any attachments, and destroy all copies.**

---

This content is for informational purposes only, should not be considered professional, financial, medical or legal advice, and no representations or warranties are made regarding its accuracy, timeliness or currency. With all information, consult with appropriate licensed professionals to determine if implementing any recommendations would be in accordance with applicable laws and regulations or to obtain advice with respect to any particular issue or problem.

Copyright © 2021 Applied Systems, Inc. All rights reserved.