

Your guide to overcoming cyberthreats

CHUBB®

Personal Risk Services



Six common cyber vulnerabilities and how to help protect the online you

Whether you're running a household or a business, you may be susceptible to cybercrime if you use the internet, computers, or other digital media. At Chubb, we look for ways to do more for our clients, like helping you prevent issues from happening in the first place. That's why we've highlighted six of the most common cyber vulnerabilities and provided tips for how you can protect your identity, your money, and your family.

1 Social media

With 3.5 billion people actively using social media - that's 45% of the world's population¹ - it's no wonder cybercriminals are targeting these networks.



Nearly
1.3 billion
social media users worldwide
have had their social media
accounts hacked in the last
five years.²

It's estimated that
50-100 million
monthly active Facebook
user accounts are fake
duplicates.⁵



How to protect yourself³

- ✓ Only share information, posts, and pictures with your inner circle—**actual friends and family**.
- ✓ **Remove yourself** from public searches.
- ✓ **Be wary of third-party apps.** While they can provide entertainment and functionality, some will also install malware and viruses on your system.
- ✓ **Use strong passwords.** Try turning a sentence into a password⁴, by using the first letter of each word in a sentence you can remember. i.e.: If your sentence is "When I was 7, my sister threw my stuffed rabbit in the toilet," your password would be "Wlw7,mstmsritt"

1 <https://wearesocial.com/us/blog/2019/04/the-state-of-digital-in-april-2019-all-the-numbers-you-need-to-know>

2 <https://www.bromium.com/wp-content/uploads/2019/02/Bromium-Web-of-Profit-Social-Platforms-Report.pdf>

3 "Social Media Prevention Tips," CyberScout

4 Bruce Schneier

5 <https://www.mcafee.com/enterprise/en-us/security-awareness/cybercriminal-social-media.html>

2 Cyberbullying

95% of teens have a smartphone and 45% say they are online “almost constantly.”⁶ It’s no surprise that bullies have taken to cyberspace.

*59% of teens have
been bullied
online⁷*



64%
*of students who
experienced
cyberbullying said it
really affected their
ability to learn and
feel safe at school.⁸*

How to protect your kids from cyberbullies

- ✓ Monitor your kids’ cell phone activity with an app like **TeenSafe**.
- ✓ Help them understand your perspective—that you are **keeping them safe**, not invading their privacy.
- ✓ **Set limits** and boundaries on their use of mobile devices.
- ✓ Lead by example—disconnect and give them **your full attention**.

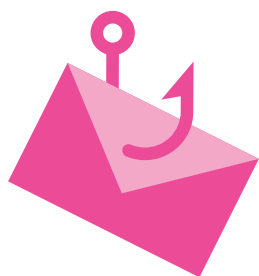
⁶ <https://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018/>

⁷ <https://pewinternet.org/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/>

⁸ <https://cyberbullying.org/new-national-bullying-cyberbullying-data>

3 Phishing scams

Most workers check email every six minutes, opening 70% of emails within six seconds of receipt.⁹ Many of these emails are phishing scams, trying to trick you into clicking on a malicious attachment or website.



More than
90%
of breaches start from
phishing emails.¹⁰

38% of malicious
email files were

**Microsoft
Office**

formats (Word,
PowerPoint and Excel).¹²



Nearly 50% of phishing
sites now use

**https
encryption,**
making them look like
they're safe.¹³

How to protect yourself¹¹

When it comes to phishing emails,
don't click the link or email itself if:

- ✓ It seems **urgent for no reason.**
- ✓ It is a request from **someone you don't know** personally or you don't do business with currently.
- ✓ You spot **poor grammar**, spelling or syntax—which means it's not coming from a reliable or professional source.
- ✓ You hover over the link and **the URL doesn't match** the description of the link.
- ✓ It asks for **sensitive information.**

9 <https://blog.rescuetime.com/communication-multitasking-switches/>

10 <https://cofense.com/>

11 "Phishing Protection Tips," CyberScout

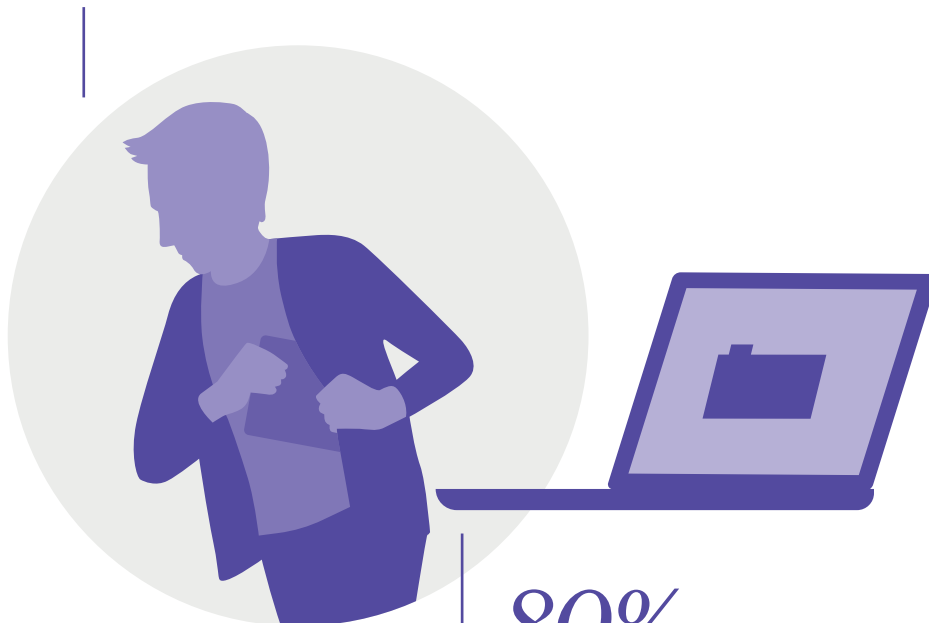
12 https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

13 <https://www.proofpoint.com/us/security-awareness/post/latest-phishing-first-2019>

4 Crimes involving electronics

These days, nearly everyone is online. That means computers and networks are a great way for cybercriminals to access your personal information or sensitive data.

*A laptop is stolen every
53 seconds¹⁵*



*80%
of the cost of a lost laptop
is from data breach.¹⁵*

How to protect your devices¹⁴

- ✓ **Password protect** every device you have.
- ✓ Install and regularly update **antivirus** and **anti-malware** security software.
- ✓ **Power down** when you're not using your computer.
- ✓ Physically **remove all storage drives** before disposing of your computer.

How to protect your network¹⁴

- ✓ **Always use encryption** (WPA or WEP) to secure your network and your wireless router.
- ✓ Set wireless to **no-broadcast**.
- ✓ **Avoid using public networks** and disable Wi-Fi access on your device when not in use.

¹⁴ "System Protection Tips," CyberScout

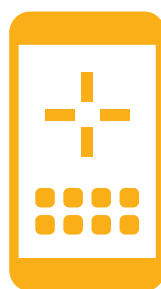
¹⁵ "Mobile Device Security: Startling Statistics on Data Loss and Data Breaches," Channel ProNetwork, <http://www.channelpronetwork.com/article/mobile-device-security-startling-statistics-data-loss-and-data-breaches>

5 Smart toys and homes

As our world becomes more interconnected, we need to look beyond the obvious cyber targets to things in our everyday lives, such as smart gadgets for the home and smart toys for the kids.

65%

of parents would pay more for a smart toy, even though smart toys can be targets for hackers.¹⁷



Routers and connected cameras represented

90% *of IoT attacks in 2018.¹⁷*

How to protect yourself¹⁶

- ✓ **Do your research**—Google the product to look for red flags about security or privacy.
- ✓ **Teach your children** what types of information are okay to share with their smart toys—and turn the toys off if they're not in use.
- ✓ Keep an eye on how your child uses the smart toy. **Turn it off** during private discussions.
- ✓ Be sure to **change the default password** and update the software regularly.

6 Ransomware

Ransomware is an attack on your computer or network that locks up or encrypts your data unless you pay a “ransom.” Experts agree that you should never pay, because you probably won’t get your data back anyway. Your best bet is prevention.

Mobile ransomware rose by

250% *in 2018.*¹⁸



It is estimated that

4,000

*ransomware attacks occur daily.*¹⁹

How to protect your yourself

- ✓ **Back up your data.**
- ✓ **Install antivirus software** and update your system regularly.
- ✓ **Never pay**—you will be giving the hackers additional information.

¹⁸ <https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf>

¹⁹ <https://www.mcafee.com/content/dam/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf>

