SAFETY CHECKLIST
POINTS OF COMPROMISE

Physical POCs
- ❑ Secure your "snail mail" (ingoing & outgoing)
- ❑ Consider paperless billing
- ❑ Opt out of "junk mail"
- ❑ Create a "wallet inventory"
- ❑ Shred unneeded documents

Technology POCs
- ❑ Carry only the cards you NEED
- ❑ Safety vs. convenience based purchases
- ❑ Minimize liability (credit vs. debit)
- ❑ Monitor your credit and bank accounts

Computers and Internet POCs
- ❑ Don't uses P2P or torrents to share files
- ❑ Keep data backed up to external drives
- ❑ Use antivirus, keep it updated
- ❑ Use VPN protocol if accessing public Wi-Fi
- ❑ Use various "strong" passwords for online accounts
- ❑ Practice "safer shopping"
- ❑ Don't fall for email or classifieds scams

Mobile Device POCs
- ❑ Physically secure your device when not in use
- ❑ Back up your data
- ❑ Minimize the amount data on the device
- ❑ Do not reply to unsolicited or suspicious texts
- ❑ Manage location settings
- ❑ Be suspicious of QRC codes
- ❑ Turn off/disable Bluetooth
- ❑ Use secure banking apps to access mobile banking (not device browser)
- ❑ Use antivirus apps and keep them updated
- ❑ Monitor permissions requested by apps

Project AWARE

Because of the complex and devastating nature of cybercrimes, we work to protect/restore victims' good names and personally identifying information. We understand the vulnerabilities associated with privacy breaches as that information is used to victimize people financially, physically and emotionally, we also understand the trauma that is created from such violations. In response to the ever-increasing demand for identity theft victim assistance, NOVA has adapted its Identity Theft Victim Assistance Summits to educate consumers right within their communities. Project AWARE is a Cyber Safety and Identity Theft Awareness program that combines innovative tools to reduce online threats and victimization, along with resources for remediation. As online fraud and identity theft victimization increase, so does NOVA's response.

About NOVA

Founded in 1975, **National Organization for Victim Assistance** is the oldest national victim assistance organization of its type in the United States. As the recognized leader in this noble cause, NOVA is a private, non-profit, 501(c)(3) organization.

Are you a victim of a crime or crisis?
Call us today. We can help.
800.TRY.NOVA or 800.879.6692
http://www.trynova.org

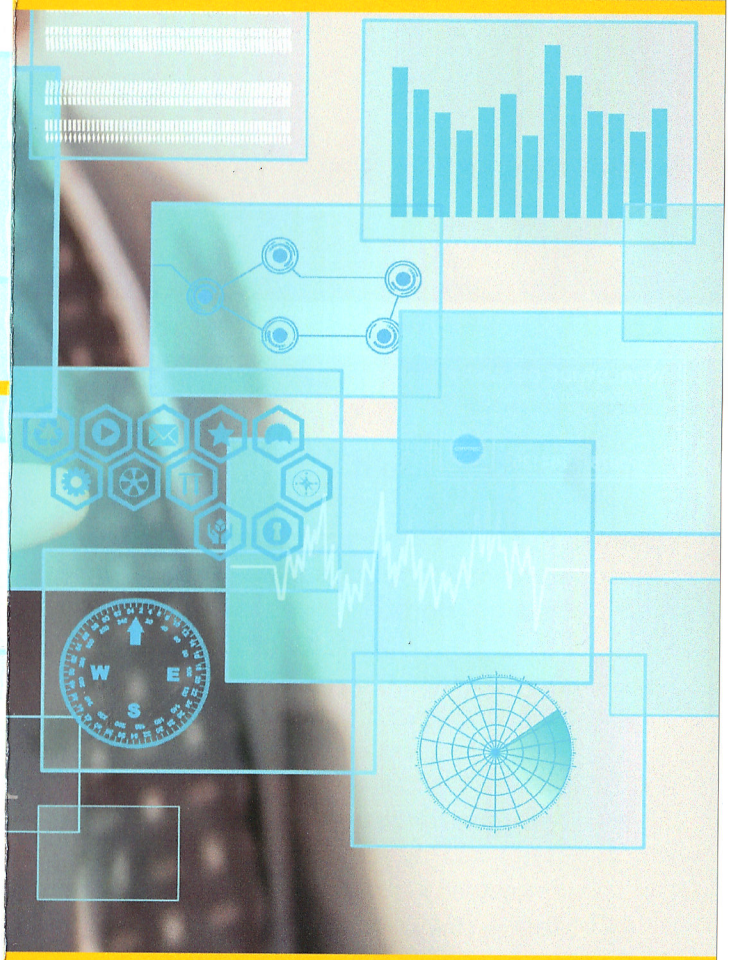
NOVA
National Organization for Victim Assistance

With support from

ATTORNEY GENERAL OF WASHINGTON

CYBER SAFETY PRINCIPLES

AWARE
CYBER SAFETY SENSE



4 CYBER SAFETY PRINCIPLES

- You are your data.
- If it has a lock, use it.
- When asked "for", ask "what for?"
- It costs more *not* to pay attention.

PRINCIPLE 1

You are your DATA

Criminals need 2 things to perpetrate cyber crime: Your **Personal Identifying Information**, and access to a **Point of Compromise**.

Examples of **Personal Identifying Information**

- Name/username(s)
- Date of Birth
- Mother's maiden name
- Address(s)
- Phone number(s)
- Email account(s)
- Passwords
- Social Security Number
- Account #(s)

Examples of **Points of Compromise**

- **Physical items**
  Examples: Dumpster diving, mail theft, check fraud, burglaries, purse/wallet snatching, shoulder surfing
- **Technology**
  Examples: Skimming, gas pumps, Point-of-Sale devices, Radio Frequency Identification (RFID)
- **Computer and Internet**
  Examples: Social Media, Email, Unsecure Websites/online shopping/classifieds, Unsecure Wi-Fi, Filesharing, BotNets, Data breaches
- **Mobile devices**
  Examples: SMShing, Geotagging, Spyware, Bluejacking, Near Field Communication, Quick Response Codes

PRINCIPLE 2

If it has a lock, use it

Secure Points of Compromise
Balance convenience vs. safety

- **Physical Items**
  Use physical locks, purge, shred, secure mail
- **Technology**
  Credit vs. debit vs. cash (PIN vs. Zip code)
- **Computer/Internet**
  STRONG Password.
  A password is a lock.
- **Mobile devices**
  Limit access,
  use password/application locks

PRINCIPLE 3

When asked FOR, ask WHAT FOR?

Practice responsible data sharing.
ASK:

- **WHY** do you need my PII?
- **WHAT** are you going to do with it?
- **HOW** will you protect it?
- **HOW** can I monitor my data?
- **WHAT** will you do when you are done with it?

PRINCIPLE 4

It costs more NOT to pay attention

An ounce of prevention is worth a pound of cure.
Safety Plan!

- Use technology to monitor and protect data
- Educate yourself on emerging technologies
- Be mindful of safety vs. convenience when accessing technology

RESOURCES FOR REMEDIATION

Federal Trade Commission
File a complaint:
877-FTC-HELP (382-4357)
http://www.ftc.gov

Identity Theft Resource Center
888-400-5530 or http://www.idtheftcenter.org

Privacy Rights Clearinghouse
http://www.privacyrights.org