

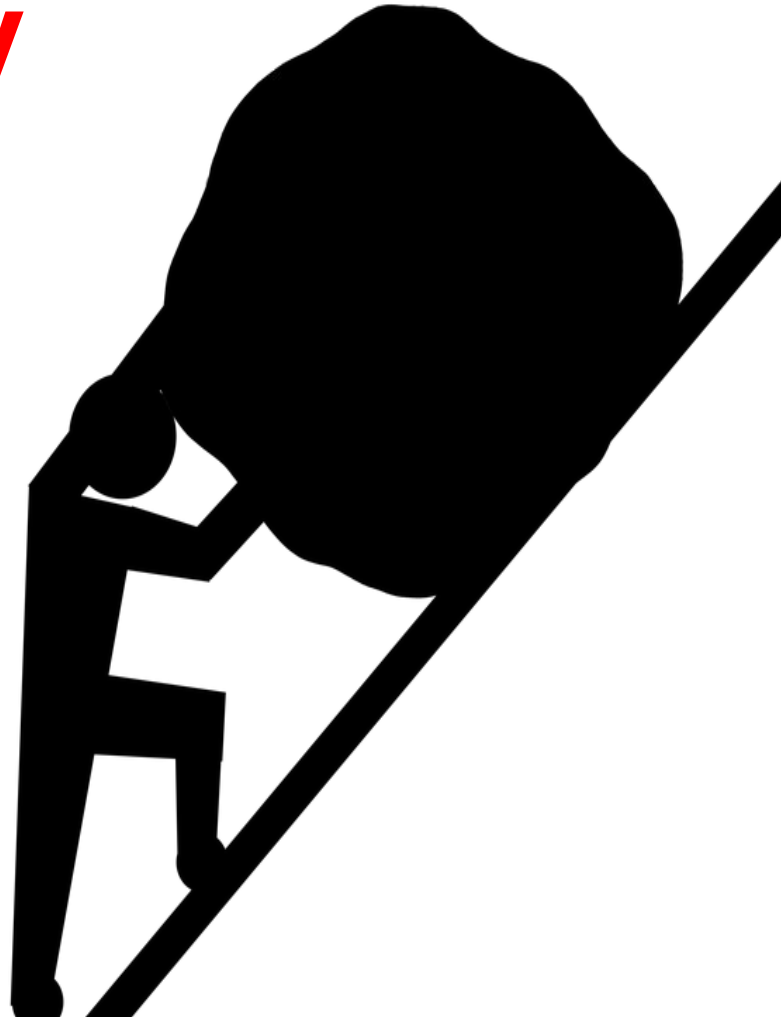
Account Security



Protecting privacy is an uphill battle

How to protect yourself online?

- Browsers
- Search engines
- Accounts & passwords
- Privacy policies and settings
- Anti-Virus & anti-malware
- Removing cookies & history data
- **Virtual Private Networks**
- Think before you type.



Password Management

What to Document in Password Log

Website Name:

Login Email:

Username:

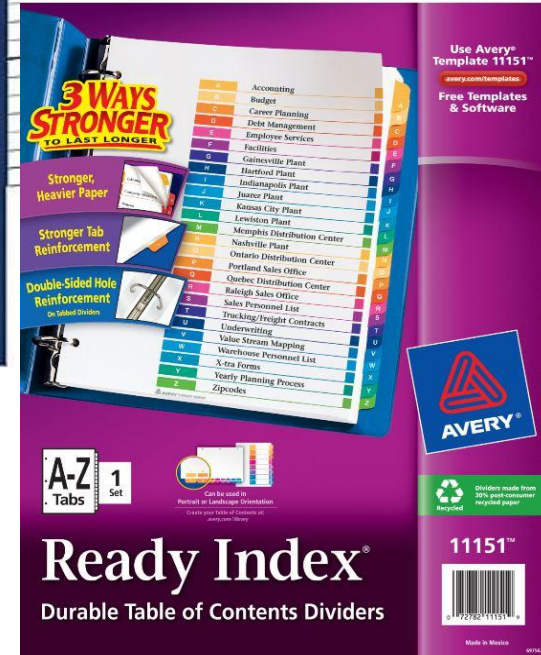
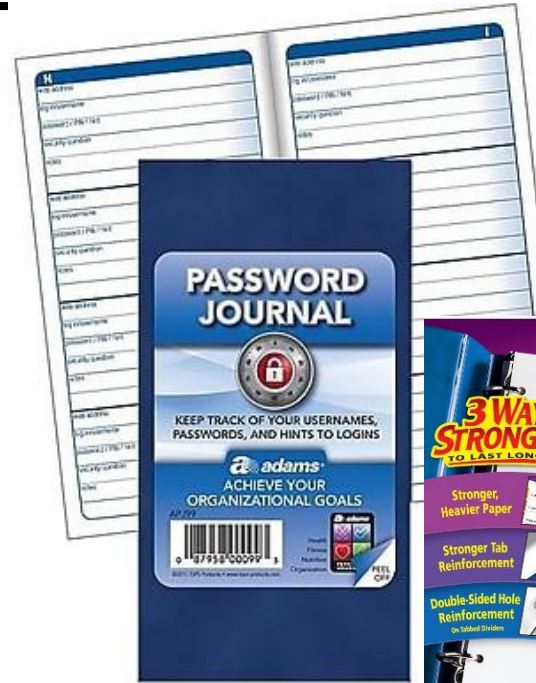
Password:

Notes:

- Is credit card on file?
- Is there downloadable content?
- What is the account for?
- Phone Number

Organize by A - Z

Write log in pencil or create a new entry when updating info.



Setting up Proof of Ownership

Security Settings

1. Adding a cell phone number (text message receiving phone)
2. Adding secondary contact email
3. Physical / Digital document of past used password and email.
4. Document of security questions and answers.

Password Recovery

1. Need access to the email and/or phone number attached to the account.
2. Password can't be recovered if you can't remember the info on the account.
3. Two-factor authentication might be accepted as proof of ownership.

Top Password Manager Software 2020

Numerous passwords and countless registration data are required when regularly using the Internet. A password must be as secure as possible and should consist of different numbers, letters, and special characters. But who can remember various of such passwords? The answer to this important question is simple: A password manager!



Password Encryption



Password generator



**Auto Form fill
function**



Password Backup



RoboForm



Avira

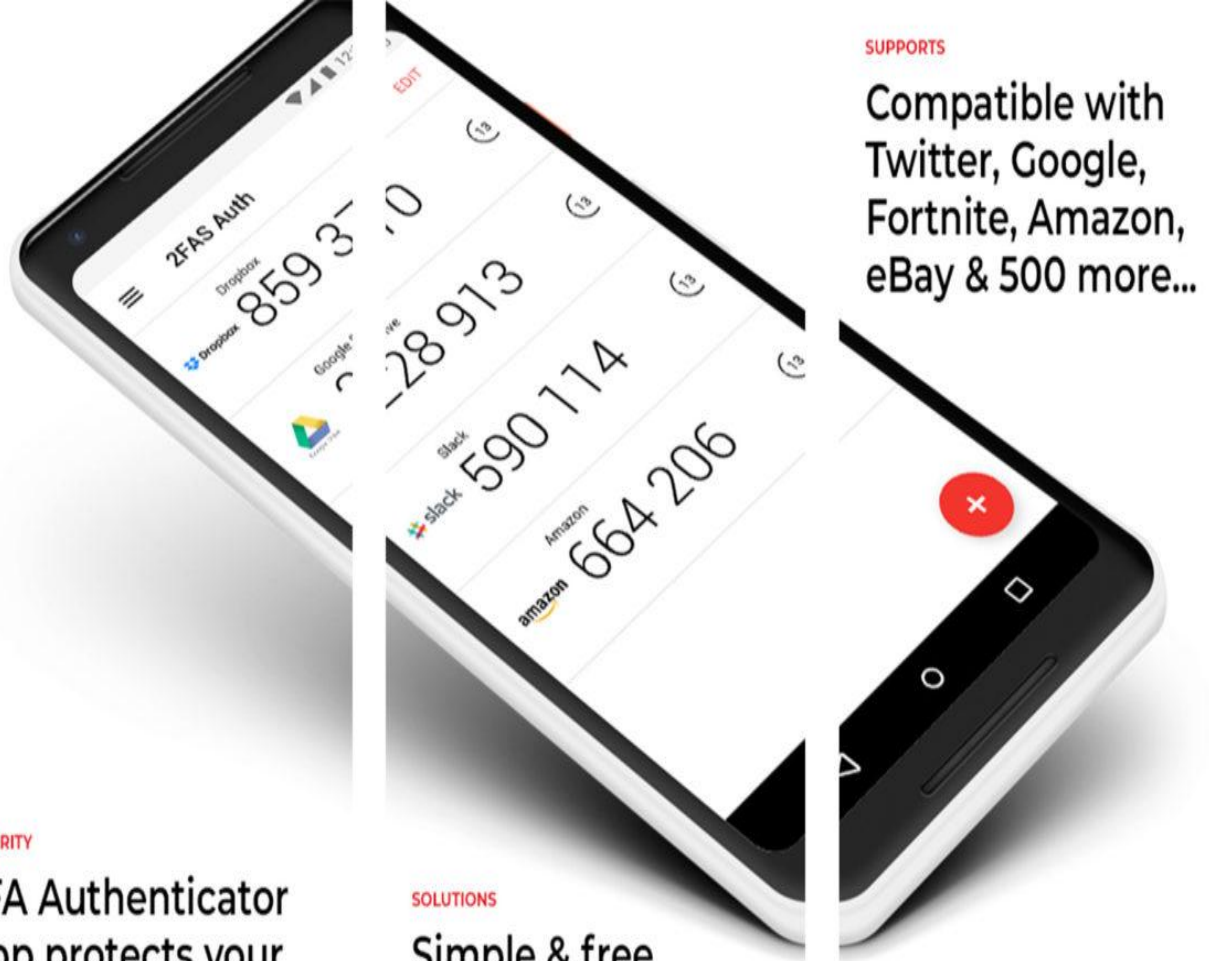


NordPass

https://www.trusted-software.com/lp/the-10-best-password-manager/?design=table&popup=y&source=gs&adw-cpn=password-c&c=2840&gclid=EAlaIQobChMIz9jE2a335wIVF4TlCh0yZg3hEAAYBCAAEgK9cPD_BwE

2 Factor Authentication Apps

- Authy
- 2FA Authenticator
- Aegis Authenticator
- Free OTP
- Google Authenticator



SECURITY

2FA Authenticator
App protects your
services & accounts.

SOLUTIONS

Simple & free
token app.

SUPPORTS

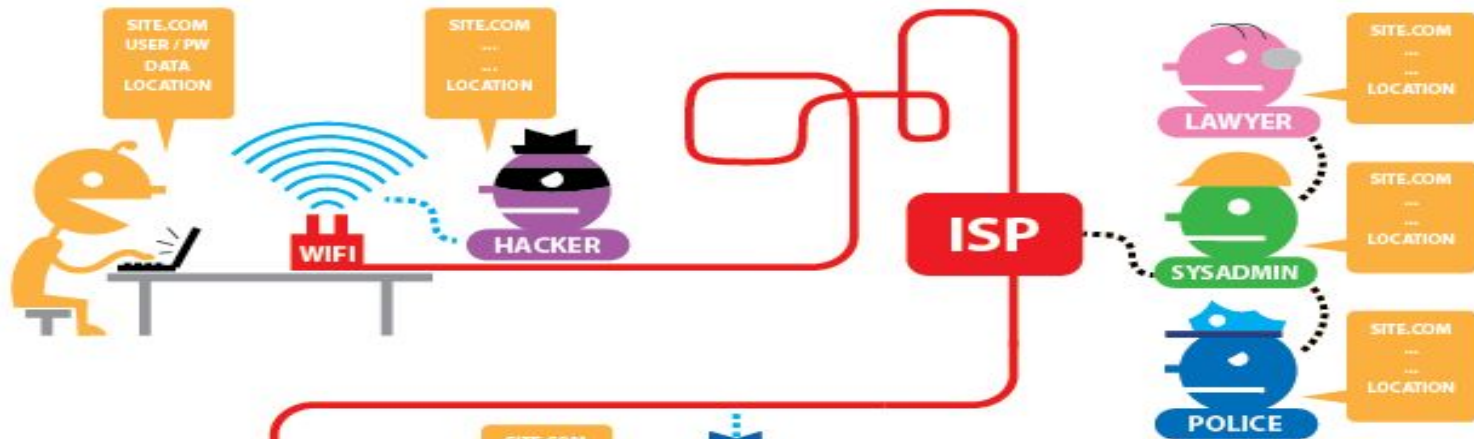
Compatible with
Twitter, Google,
Fortnite, Amazon,
eBay & 500 more...



Video Name: Using 2-step verification

Video Creator: Google

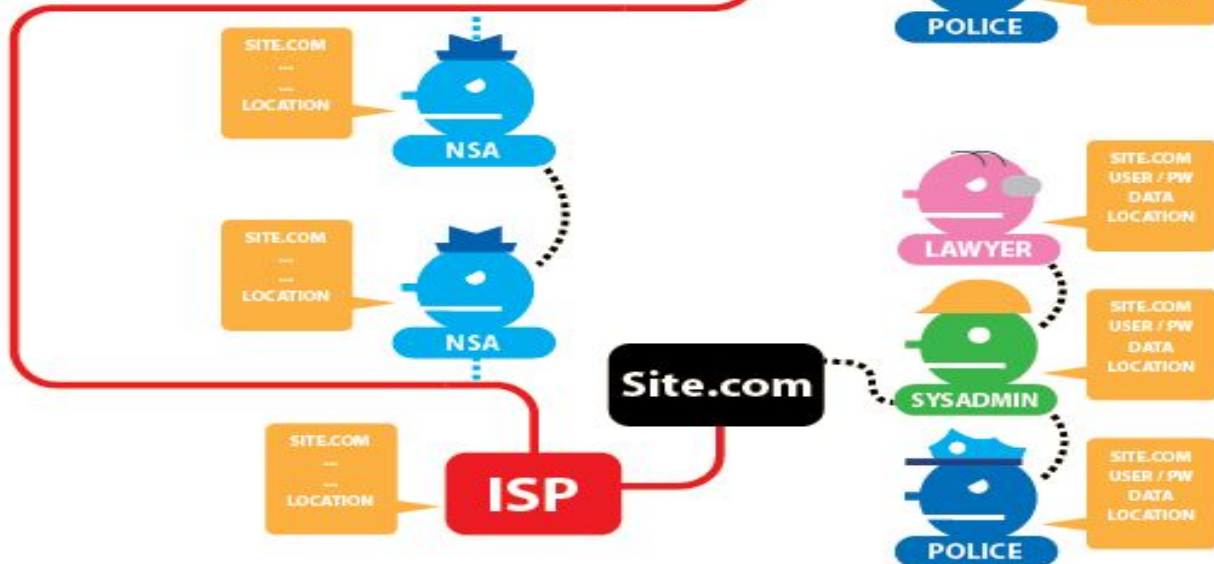
Website URL: <https://www.youtube.com/watch?v=zMabEyrtPRg>



Internet Service Provider

System Administrator

- Creators of the website or service.



KEY

Internet connection ————

Eavesdropping - - - - -

Data sharing



YouTube Video Name:

What is a VPN? How it works and why you should get one

YouTube Channel:

All Things Secured

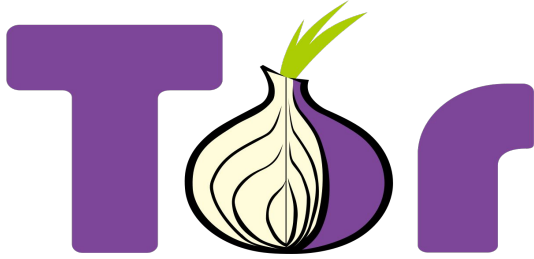
Website :

https://www.youtube.com/watch?v=gX1nM_p0m0I

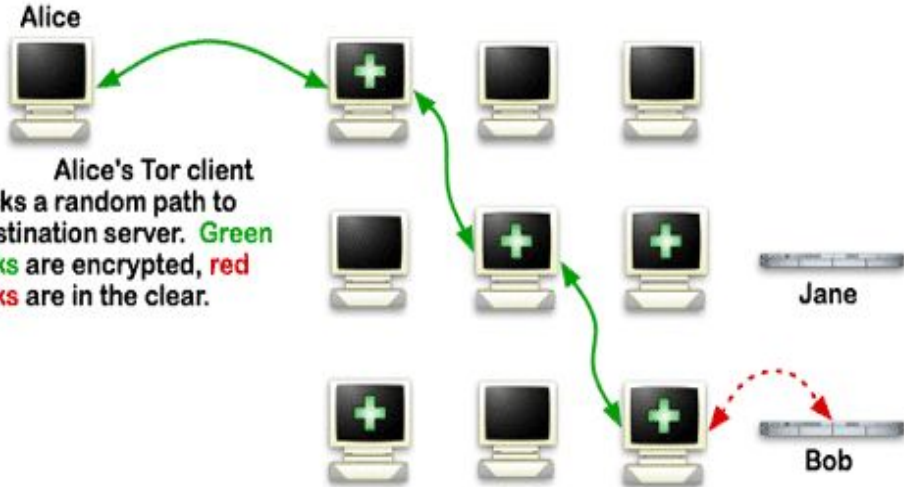
1. Nord VPN
2. Private Internet Access VPN
3. Tunnel Bear VPN
4. CyberGhost VPN
5. Express VPN
6. IPVanish VPN
7. Tor Guard VPN
8. Surfshark
9. Norton Secure VPN
10. Proton VPN

<https://www.pcmag.com/picks/the-best-vpn-services>

Private Web Browsers



How Tor Works

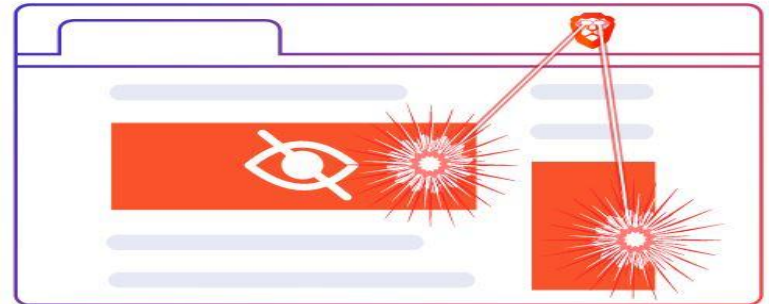


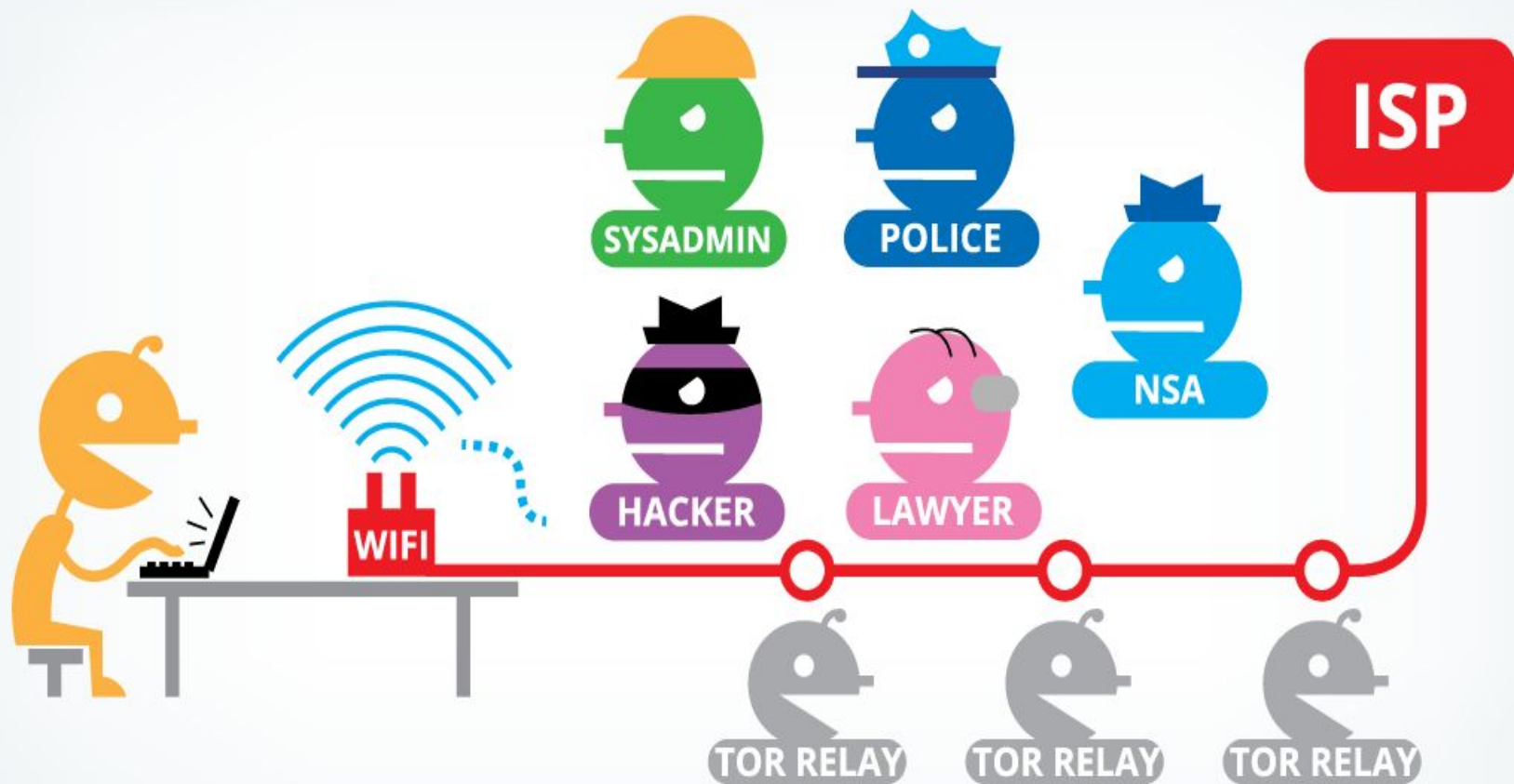
Brave Shields for Privacy

Block data-grabbing ads and trackers

The vast bulk of websites and ads include software that tries to identify you. They want to track your every move across the web. Brave blocks all this, allowing you to browse freely.

[Learn more about Brave Shields](#) →





SECURED WEB SEARCH



Non-Logging Search Engines

1. **Startpage:**
Uses Google technology without the tracking, to provide an anonymous and smooth browsing experience.
2. **DuckDuckGo:**
Most well known private search tool, offers a 100% transparent privacy policy.
3. **Swisscows:**
Uses privately owned servers, and collects search results from multiple engines.
4. **Searx.me:**
Meta search engine that runs on open source software and encourages you to modify their code for ultimate security.
5. **Disconnect Search:**
Results are displayed in the style of the search engine they were taken from.

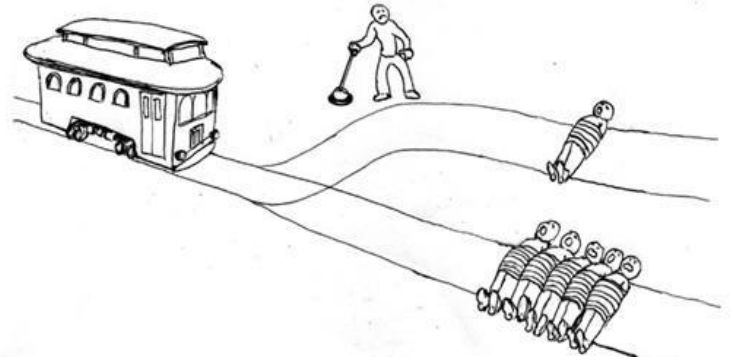
<https://www.vpnmentor.com/blog/best-private-search-engines-true-no-log-services/>

Secure Yourself



Keep vigilant of new risks.

Stay careful of gullible actions / choices.



Be aware of your online presence & actions.

S

Stay Safe

Don't give out your personal information to people / places you don't know.



M

Don't Meet Up

Meeting someone you have only been in touch with online can be dangerous. Always check with an adult you trust.



A

Accepting Files

Accepting emails, files, pictures or texts from people you don't know can cause problems.



R

Reliable?

Check information before you believe it. Is the person or website telling the truth?



T

Tell Someone

Tell an adult if someone or something makes you feel worried or uncomfortable.

Follow these SMART tips to keep yourself safe online!



Stay Safe

Don't give out
your personal
information to
people / places
you don't know.



- Keep all passwords secret, always use strong passwords.
- Don't needlessly disclose your date of birth, mother's maiden name, favourite pet's name, online.
 - These and similar are often used as basic security questions when you forget details of online accounts as proof of identity.
- If using a social media website always check the privacy settings for your account. Always think before sending messages and post.
- Be aware of email and instant **messaging threats**, remain vigilant against **phishing scams** and make sure that all computers you use are secure and free from **spyware**.
- Keep your computer storage media safe from theft or loss
- If disposing of computer, wipe all hard drives or other storage media using a specialist software tool
 - (just formatting the drive is not enough)

M

Don't Meet Up

Meeting someone
you have only
been in touch
with online can be
dangerous.
Always check with
an adult you trust.



5 Reasons to be Cautious

1. Internet Trolls & Bullies
 - a. Someone who goes out of their way to harass, bully or upset others.
 - b. Catfishing is the act of promising to meet someone from online and not showing up to meet.
 - i. Most people who catfish use a false photo and identity.
2. Identity Theft
 - a. Talking to someone in a personal conversation could leave your guard down to revealing information including
 - i. Full Name
 - ii. Age
 - iii. Address
 - iv. Friends and Family
3. Images
 - a. Private images could be shared or be used against you.
4. Online Personality \neq Real Attitude
 - a. Text and emoji don't convey tone and attitude.
 - b. Some might write in a way that might be interpreted incorrectly.
5. Abuse, Robbery, and ulterior motives.

1980's

Don't get into
cars with
strangers

1990's

Don't talk to
strangers on the
internet

2000's

Summon a stranger from
the internet and get into
their car



Emotional Tactics

Signs of a Scam



Professes love quickly.
Claims to be from the U.S.,
but is overseas for business
or military service.



Asks for money, and lures
you off the dating site.



Claims to need money
— for emergencies,
hospital bills, or travel.
Plans to visit, but can't
because of an emergency.

What to do

- 1 Slow down** — and talk to someone you trust. Don't let a scammer rush you.
- 2 Never wire money**, put money on a gift or cash reload card, or send cash to an online love interest. You won't get it back.
- 3 Contact your bank right away** if you think you've sent money to a scammer.
- 4 Report your experience to:**
 - The online dating site
 - Federal Trade Commission: [ftc.gov/complaint](https://www.ftc.gov/complaint)
 - Federal Bureau of Investigation: [ic3.gov](https://www.ic3.gov)

Green Dot Card Scam.

The Scam.

People are losing thousands of dollars in a phone scam involving Green Dot MoneyPak cards. After receiving a call from someone who claims to be collecting a debt from either a Utility Company, the IRS or as settlement for an auto accident; people are being threatened with the loss of their heat, electric, possible deportation or criminal prosecution. Three typical scenarios:

- IRS Scam --** A caller informs the victim that they owe back taxes to the IRS and must make immediate payment with a Green Dot Money-Pak.
- Accident Scam --** The victim's family member had a car accident and the caller threatens physical violence unless immediate reimbursement is made with a Green Dot Money-Pak.
- Utility Scam --** Utility companies demand immediate payment by Green Dot Money-Pak or your electricity or gas will be turned off.

What Can I Do?



Caution

Be suspicious of callers who demand immediate payment for any reason.



Information

Never give out personal or financial information to anyone who emails or calls you unsolicited.



Know Them

Never wire money, provide debit or credit card numbers or Green Dot Money-Pak card numbers to someone you do not know.



Know This

Utility companies and government agencies will not contact you demanding immediate payment by Money-Pak.



Report It.

If you can not verify the I.D., feel unsafe, or suspect criminal activity, call 911 immediately.



Remember

Remember that anyone who has the number on a Green Dot Money-Pak card has access to the funds on the card.

NYPD



Prevent harmful file downloads

- Only download from sites you trust
- Be careful of email attachments and website links.
- Only download from companies you trust.
- Never download illegally obtained media
- Scan your downloads
 - Anti-malware tools can quickly scan a file or download and its tell you of any **known** viruses or harmful software.
- Backup your computer
 - Every three months make sure your files are saved on another device.
 - Use a cheap laptop or tablet to browse the internet and a different computer for saving important files.



Video Name:

Protect Your Computer from Malware

Video Creator:

FTCvideos

Website URL:

https://www.youtube.com/watch?v=XU8PHihT_P4

Signs that a website is authentic:

- Website policy & agreement
- Third party website reviews
- Privacy statement
- Contact info
- Are the prices / product realistic?

Check the website for SSH Authentication

If it begins with “https” instead of “http” it means the site is secured using an SSL Certificate. **SSL Certificates** secure all of your data as it is passed from your browser to the website’s server.

To get an SSL Certificate, the company must go through a validation process.



R

Reliable?

Check information
before you believe
it. Is the person
or website telling
the truth?





Tell Someone

Tell an adult if
someone or
something makes
you feel worried
or uncomfortable.

In general, the police are more likely to be able to help in some way with the following forms of online harassment:

- You've received or been named in direct threats of violence (ie: threats that suggest a time, place, or location are more likely to be taken seriously by law enforcement)
- An online abuser has published nonconsensual, sexually-explicit images of you.
- You've been stalked via electronic communication.
- You know your online harasser and wish to seek a restraining order.

These are by no means the only reasons you might wish to turn to law enforcement for help. Even if reporting online harassment to your local precinct doesn't result in immediate action, at the very least, it will establish a paper trail that might be needed later on.

The **federal stalking statute**, for example, has been amended to include the use of "any interactive computer service or electronic communication service . . . to engage in a course of conduct that . . . causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress" to the targeted person or persons.

Consult with a lawyer in the correct field before any legal proceedings.

Presenters Personal Option

1. **Your data is worth money \$\$**
 - a. Is giving your personal data worth giving away for a luxury gimmick?
 - b. Is it fair that you paid for a product then the seller gets more money for selling your info?
2. **Your face, your ID, your voice**
 - a. If it is searchable in your name or photo than take responsibility for it. Facebook posts, tweets, and comments on a webpage.
 - i. People are getting fired for “Trending” for being rude on camera / recording..
3. **Internet Search can be used against you in court.**
 - a. Based on the crime & company the police might obtain your search history.

Why Online Privacy is Important

Examples:

Bullied dead girl's image used in dating ad on Facebook

<https://www.nbcnews.com/technolog/bullied-dead-girls-image-used-dating-ad-facebook-4B11187466>

I
STOP
BEFORE
I

POST ON
SOCIAL MEDIA



STOP | THINK | CONNECT™

www.STOPTHINKCONNECT.ORG



I
think
BEFORE I

TYPE MY INFORMATION



STOP | THINK | CONNECT™

www.STOPTHINKCONNECT.ORG



MY PASSWORD
MIXES
LeTtERs
#umbers
AND
\$ymbol!#



STOP | THINK | CONNECT™

www.STOPTHINKCONNECT.ORG

