Quote: It's not that I have anything to hide, it's that I have nothing I want to show you!

Why is it assumed that you must have something reprehensible to hide if you are hiding stuff, that’s like a peeping tom and if you close the drapes, you have something nefarious to hide. The real attitude should be You See Nothing about me, unless I choose to show you something.

Privacy and security on the internet are entwined. Privacy helps with your security and security helps with your privacy. For example, if they don’t know your bank, then it makes it hard to target your bank. The opposite would be true, except US law requires that banks know you. But what about your local furniture store? Should they know your home address, and birthday? What will hackers gain if that hacked that store? Would it provide them with knowledge of where you live, and they expensive TV you bought, making you a target?

Did you create an account at some online location and with your email and your standard password. Was that location was hacked, and now the hackers have the same email and password you use with your bank? They don’t even have to your bank, they just drop your email and password into their app which tries all the banks.

Addressing these is the reason I am developing this section. Things you can do on the internet to be safer and more private.

Emails:

Use multiple emails. Have a personal email account for friends and family. Have a different email for financial institutions. Have a throw away emails for sites that require an email to download information but you doubt you will ever use again. Your friends will have your email in their contact list. But if they get hacked, the bad guys don’t have your financial institution emails. The throw away email can be thrown away every year, because you have no intention of going back to the site, yet you know they sold your email to spam sites. I am carried away with this. I have different emails for Amazon, Microsoft, Google, Facebook, financial institutions, and annual throw away emails. For example, if you give an email address to an insurance quote site, you will receive hundreds of spam emails. There are several ways to accomplish this. And don’t allow your email to be publicly visible on any web page. Web crawlers will find it and add to the spam list. Best email providers …

Browsers:

Do you think an InPrivate/Anonymous/incognito mode of your browser is safe, then think again. If you were using Chrome, google was tracking you anyway. When you accessed a site, they didn’t know who you were, until you sigh in. If you accessed a different site without closing the browser first, that new site has the ability to know the previous site you were on by use of cookies and other techniques. There is also browser fingerprinting which can identify you even if cookies were cleared or you were using a VPN. Best browser choices are Firefox, and Brave. Look up how to change your default search engine on the browser to something like DuckDuckGo. Even better is to use different browsers for different jobs.

VPN:

A VPN will change the location of your entry point into the internet, but it won’t hide your activity from that point on. Also, your VPN has the ability to monitor everything you do, so pick a VPN that does not keep logs and has a history of protecting users. Always use a VPN if connecting over any public WiFi in coffee shops, airports, even your hotel rooms. There are technologies which hackers can use to intercept your access and present fake banks.

Passwords:

Is your password actually your name backwards with a number which you increment every time you are forced to change your password? Is so, bad choice. So how do you manage complex passwords, and keep unique password among each site? If you keep your password in a file on your machine called something like passwords.list, when the hacker scans your machine, they got you. Also, when your machine crashes (or gets stolen), you lose your passwords. A password manager is your key to solve these problems. My passwords look like this: “iq&6HH!59aYNL%” or this: “!BiiKPpZy47sX8”? They are not only unguessable, but I can’t even type them in correctly. I use a password manager that run in my browsers, and on my phone. It fills in the userid and passwords for me. For security, it also won’t fill in the userid and password if the site is incorrect. If some hacker created a web that looked like Bank Of America but used a Chinese character for the ‘o’ which looks like an ‘o’ on our computers, the password manager will not insert the credentials.

Is your password something line your name spelled backwards with a number which is incremented every time you are forced to change your password?

        Is so, bad choice.

        So how do you manage complex passwords, and keep unique password among each site?

        Do you keep a file on your computer with password, called passwords.list, when the hacker scans your machine, they got you.

        Or, when your machine crashes (or is stolen), you lose your passwords.

        A password manager is your key to solve these problems.

        My passwords look like this: “iq&6HH!59aYNL%” or this: “!BiiKPpZy47sX8”.

        They are not only unguessable, but I can’t even type them in correctly.

        I use a password manager that run in my browsers, and on my phone.

        It fills in the userid and passwords for me.

        For security, it also will not fill in the userid and password if the site is incorrect.

        Even if some hacker created a web that looked like you bank, but they used a foreign character than translates to a US letter but is really different.

        The password manager will not insert the credentials.

What to look for in a password manager: (1) stored in the cloud, accessible from all your machines. (2) MFA for access so no one else has access to your passwords. (3) Zero-Knowledge. Then means that the company you use cannot see your data even if they are hacked or have a corrupt employee. (4) privacy oriented with reporting (Lastpass failed this step, they were hacked and didn’t tell anyone) (5) Open source is good. Anyone who can read a program can verify their code is not corrupt. Best password managers on the market today are Bitwarden, ProtonPass and 1Password. Bitwarden and Protonpass have a free version for basic password functions. 1Password is supposed to be easiest to use. I use Bitwarden, the paid version because it will also manage Passkeys, the newest technology for securing access to your sites. If you are extremely geekish, you can download Bitwarden and set it up on your secure NAS instead of relying on Bitwarden’s cloud.

Apple’s new password manager is limited to Apple devices and I am not sure they even implement zero-knowledge architecture.

Browser based password storage is limited to the browser and they are a lot of tools out there to hack those passwords. Don’t save passwords in a browser.

About MFA:

When you bank decides they need to verify it’s really you, they are likely to send you a code to your phone. This is a form of MFA. Sim Swapping is where someone takes over your SIM, which is access to your phone number. Once done, the bank sends a code to your phone and the hackers has access to your bank account. The banks know this happens, but they don’t implement better security.

Better MFA is technology like TOTP which is pretty unique, authenticator app which is a way of implementing TOTP, hardware key like Yubikey, and the new Passkey technology.

TOTP and authenticator apps are time based. Based on a starting point which is unique to you and the web site, this generates a new unique code for you every 30 seconds. The web page knows the same starting point and will compare the number you provide with what they expect for you. The main weakness about TOTP is the authenticator app you use and Phishing attack on you. You can get an app from Google, Microsoft , Authy. Apple has one, but it locks you into the Apple ecosystem. Using Google’s or Microsoft’s app means it exist wherever you are logged in. That means they know where you go, limiting your privacy and is someone hacks your account, they have your access. I don’t know anything about Authy. I use Bitwarden’s TOTP authenticator app.

Yubikey is a hardware key. When it’s required, you plug the key into your device, or connect via NFC, and Yubikey verifies this is you. A web site ask for your password then it ask for the key, thus there are two factors, something you know (password) and something you have, (the key). The down side is the cost, of both the Yubikeys at around $50 each. You need a backup key in case you lose the main key. That also means you need to set up both keys when you apply them to a site. I used Yubukey as MFA to protect my Bitwarden account which has my passwords and TOTP data. I keep one in my house and the other at a location I can get to if my house Yubikey burns down or the house key is stolen.

Passkeys is the newest tech to protect your accounts. It’s based on extremely secure codes which a web site can use to verify your device is authorized to access that site. The problem is about your ‘device’. Passkeys on your device could be Windows Hello login. Or it could be secured on your phone. In both cases, lose that ‘device’ and you lose access. You need a Passkey manager that follows you and is secure. Apple iCloud Passkey might follow you around within the Apple ecosystem and has problems outside of their ecosystem. Google already knows too much about you, do you want them to know your Passkeys also? What if someone hacks your google account? For me, I use Bitwarden’s Passkey manager.

Secure with Bitwarden

If you read this far, you can see I use Bitwarden for passwords, TOTP and Passkeys. Bitwarden, and I suspect, all password managers run in the browser, and on the phones. In the browser, it will open the page and fill in the userid and password. If TOTP is required it’s a click away. If Passkey is required, Bitwarden ask me if it’s OK to supply a Passkey. Bitwarden has zero knowledge out side of my machines. If I was using a password like: “MySecretPassword” Bitwarden only receives stores something like: “U2FsdGVkX1/nm1XL4XYhyR2kkSOhtKzQM9XaZpHDb81n57baOdg9fX03K5UrdpOJ” Without my userid (a different email than my normal activities) and my password and my Yubikey, you would need a quantum computer to figure out my password. And quantum computers don’t really exist yet.

Any password of the good password managers works like this. This includes Protonpass and 1Passwrod and, maybe Nordpass. I’m sure others are just as good.

Privacy and Security reference: <https://www.youtube.com/watch?v=XNOAOQktG6U>

Pass 1

Internet Security and Privacy: Protecting Your Digital Life

It's not that I have anything to hide, it's that I have nothing I want to show you!

In today's interconnected world, internet security and privacy are paramount. The common misconception that only those with something to hide need privacy is fundamentally flawed. Instead, the principle should be: "You see nothing about me unless I choose to show you something."

The Interplay of Privacy and Security

Privacy and security on the internet are closely intertwined, each reinforcing the other. For instance, keeping your banking information private enhances your financial security

1

.

Key Areas of Concern

**Email Management:** Utilize multiple email accounts for different purposes:

* Personal email for friends and family
* Separate email for financial institutions
* Disposable emails for one-time registrations

This strategy minimizes the risk of compromising sensitive information if one account is breached

1

.**Browser Safety**

* Private browsing modes are not as secure as many believe
* Consider using privacy-focused browsers like Firefox or Brave
* Change your default search engine to privacy-respecting alternatives like DuckDuckGo
* Use different browsers for different activities to compartmentalize your online presence

1

**Virtual Private Networks (VPNs)**While VPNs can mask your location, they don't guarantee complete anonymity. Choose a VPN provider that:

* Doesn't keep logs
* Has a history of protecting user privacy
* Is especially crucial when using public Wi-Fi networks

1

**Password Security**Strong, unique passwords are essential for each online account. Password managers offer a solution by:

* Generating complex, unguessable passwords
* Securely storing credentials
* Auto-filling login information on verified sites

Top password managers include Bitwarden, ProtonPass, and 1Password

1

.

Multi-Factor Authentication (MFA)

MFA adds an extra layer of security beyond passwords. Consider these options:

* Time-based One-Time Password (TOTP)
* Authenticator apps
* Hardware keys like YubiKey
* Passkeys, the newest secure login technology

1

Implementing a Comprehensive Security Strategy

For optimal security, consider using a combination of tools:

* A reputable password manager for credential storage
* TOTP for additional authentication
* Hardware keys for critical accounts
* Passkeys for supported services

By adopting these practices, you can significantly enhance your online privacy and security, protecting your digital life from potential threats

1

.

<h2>The Interconnection of Privacy and Security Online: Protecting Your Digital Life</h2>

<i>It's not that I have anything to hide, it's that I have nothing I want to show you! </i>

<h3>The Symbiosis of Privacy and Security</h3>

Privacy and security on the internet are inextricably linked, each reinforcing the other in a symbiotic relationship

Consider how privacy enhances security: if malicious actors are unaware of which bank you use, it becomes significantly more challenging for them to target your financial assets. While the inverse relationship is somewhat limited by legal requirements—U.S. law mandates that banks verify their customers' identities—the principle still applies in many other contexts.

For instance: Consider your local furniture store. Should they possess sensitive details such as your:

* Home address
* Date of birth
* History of items bought

The risks associated with oversharing become apparent when we consider potential data breaches.  If hackers were to compromise such a store's database, they could gain access to:

1. Your residential location
2. Information about high-value purchases, such as expensive televisions

This combination of data could potentially make you a prime target for burglary or identity theft. By carefully managing the information we share with various entities, we can significantly reduce our vulnerability to cyber threats. This underscores the critical importance of maintaining privacy as a cornerstone of our overall online security strategy.

<h3>Critical Areas of Focus</h3>

<h4>Email Management</h4>

<p>Utilize multiple email accounts for different purposes:

<ul>

<li>Personal email for friends and family</li>

<li>Separate email for financial institutions</li>

<li>Disposable emails for one-time registrations</li>

</ul>

<p>This strategy minimizes the risk of compromising sensitive information if one account is breached.</p>

<h4>Browser Safety</h4>

<p>Consider the following for safer browsing. Private browsing modes are not as secure as many believe, your information is not sent to a web site but the browser vender may still have it. While an initial private session has no cookies, as your browser cookies are collected. Cookies and browser fingerprinting provide tracking information. </p>

<ul>

<li> </li>

<li>Use privacy-focused browsers like Firefox or Brave</li>

<li>Change your default search engine to privacy-respecting alternatives like DuckDuckGo</li>

<li>Use different browsers for different activities to compartmentalize your online presence</li>

</ul>

<h4>Virtual Private Networks (VPNs)</h4>

<p>While VPNs can mask your location, they don't guarantee complete anonymity. Choose a VPN provider that: </p>

<ul>

<li>Doesn't keep logs</li>

<li>Has a history of protecting user privacy</li>

<li>Is especially crucial when using public Wi-Fi networks</li>

</ul>

<div>

Public WiFi Security Risks and VPN Protection

Public WiFi networks, commonly found in coffee shops, airports, and hotels, pose significant security risks to unsuspecting users. These seemingly convenient connections can harbor hidden dangers, primarily in the form of Man-In-The-Middle (MITM) attacks.

The Threat of MITM Attacks

When connected to public WiFi, users are vulnerable to MITM attacks, where malicious actors intercept communications between the user and the intended recipient. This interception allows cybercriminals to:

* Capture sensitive personal information
* Steal login credentials
* Monitor online activities

VPN: A Shield for Public WiFi Users

To mitigate these risks, cybersecurity experts strongly recommend using a Virtual Private Network (VPN) when accessing public WiFi networks. A VPN offers several key benefits:

1. **Encryption**: VPNs encrypt your data, making it unreadable to potential interceptors.
2. **Anonymity**: Your IP address is masked, enhancing your online privacy.
3. **Secure connection**: VPNs create a secure tunnel for your data, bypassing potential threats on the public network.

By employing a VPN while using public WiFi, users can significantly reduce their exposure to MITM attacks and other cybersecurity threats, ensuring a safer online experience in public spaces.

</div>

<h4>Password Security</h4>

<p>Strong, unique passwords are essential for each online account. Password managers offer a solution by:<sup><a href="#fn1" id="ref6">1</a></sup></p>

<ul>

<li>Generating complex, unguessable passwords</li>

<li>Securely storing credentials</li>

<li>Auto-filling login information on verified sites</li>

</ul>

<p>Top password managers include Bitwarden, ProtonPass, and 1Password.</p>

<h3>Multi-Factor Authentication (MFA)</h3>

<p>MFA adds an extra layer of security beyond passwords. Consider these options:<sup><a href="#fn1" id="ref7">1</a></sup></p>

<ul>

<li>Time-based One-Time Password (TOTP)</li>

<li>Authenticator apps</li>

<li>Hardware keys like YubiKey</li>

<li>Passkeys, the newest secure login technology</li>

</ul>

<h3>Implementing a Comprehensive Security Strategy</h3>

<p>For optimal security, consider using a combination of tools:<sup><a href="#fn1" id="ref8">1</a></sup></p>

<ul>

<li>A reputable password manager for credential storage</li>

<li>TOTP for additional authentication</li>

<li>Hardware keys for critical accounts</li>

<li>Passkeys for supported services</li>

</ul>

<p>By adopting these practices, you can significantly enhance your online privacy and security, protecting your digital life from potential threats.</p>

<hr>

<ol class="footnotes">

<li id="fn1">Internet Security and Privacy Document. <a href="#ref1">↩</a> <a href="#ref2">↩</a> <a href="#ref3">↩</a> <a href="#ref4">↩</a> <a href="#ref5">↩</a> <a href="#ref6">↩</a> <a href="#ref7">↩</a> <a href="#ref8">↩</a></li>

</ol>