# Protecting Your Accounts and Identity From Theft

WordCamp NYC 2019

Chin ~ ConsciousVibes.com

## Data Breaches

Data Breaches Exposed 4.1 **B**illion Records in the First Six Months of 2019!

## Data Breaches

Data breaches have exposed names, addresses, passwords, PINs, social security numbers, credit card information, etc.

## Data Breaches

Data analysis and less expensive computing power make it trivial to combine information from several data breaches.

### Data Breaches

Stolen credentials are as valuable as cash to cybercriminals. Whether they sell the stolen data or use it to takeover accounts, a single data breach can result in years of profit if cybercriminals

### Phishing Attacks

In addition to data breaches, phishing attacks are becoming increasingly sophisticated and that’s just the tip of the iceberg.

### Trivial Cell Phone Hack

SIM-swap attacks, are where someone uses pieces of personal information to convince your cell service provider to transfer (port) your number and associated phone account to a device in the attacker's possession.

### Bad Password Hygiene

The problem with stolen credentials, which is the number one cause of compromised accounts every year, stems from Internet users using the same, or similar, passwords across multiple accounts.

## Good Password Hygiene

Generate new strong passwords for all your accounts and use a password manager to store your passwords.

Make sure to use a very strong passphrase to access your password manager.

## Best Practices

Enable MFA/2FA on all accounts that have that option.

An authenticator app is preferred over text/SMS messages.

## Best Practices

Do NOT let operating systems, browsers, or your Google Account save your passwords.

## Best Practices

Do NOT click links or open attachments in unsolicited e-mails.

It could be an attempt to phish you, or install malware on your system.

## Best Practices

Create a new e-mail account that you never use to login anywhere.

Then set the new e-mail address as your recovery e-mail address for all your accounts.

## Best Practices

When you set up responses to security questions on Web sites, do NOT use information that may have been exposed in a data breach.

## Best Practices

Never give out personal, banking information, or passwords in response to an unsolicited phone call, e-mail, text message or fax, even if the caller or sender identifies themselves as being from a trusted source, like your bank or credit union.

## Best Practices

Make sure that all your devices, operating systems, and software applications are fully patched and up-to-date.

## Best Practices

Follow the Principle of Least Privilege by never running as an administrator/root user unless absolutely necessary.

## WordPress

Create a user account, whose role is an editor, for your day-to-day use.

Minimize using the Admin account.

## WordPress

Don’t give developers your Admin credentials.

Have them register as a Subscriber, then change their role when necessary.

One cannot escape the fact that, data breaches have already exposed your personal information, and will continue to happen.

Make the effort to understand, implement, and share what you've learned to protect yourself, and others, from the fallout of data breaches, phishing attacks, and identity theft.

## Your Time is Valuable

Reduce the risks from compromised accounts by implementing as many layers of protection that you can, by following follow Best Practices.

# Protecting Your Accounts and Identity From Theft

WordCamp NYC 2019

Chin ~ ConsciousVibes.com