VICTORY INVESTIGATIONS

Data Privacy Awareness Tips

Text, email, voice

1

Be cautious of phishing, smishing, & vishing attacks...

Phishing, smishing and vishing are all common social engineering tactics that are used to steal confidential data. The difference between these scams are how the cybercriminals contact you by email, text, or phone. These types of attacks are dangerous as the malicious actor acts as a reputable company or trusted person, so it is more likely you fall for the scam.

Never click on unknown links!

Use this VPN for added protection.

2

https://

Protect Your Web Browsing...

If you need to send sensitive or confidential information on the web, always check that the website is secure. To know if a website is secure, you can view the URL. A secure website will begin with “https://” and have a lock icon. This means the data you send and receive is encrypted in transit. This will prevent malicious actors and unauthorized parties from viewing what data is being sent. Even if a URL starts with “https://” you should always verify that the website is legitimate before entering data..

Pro Tip: Using a reputable password manager can help.

3

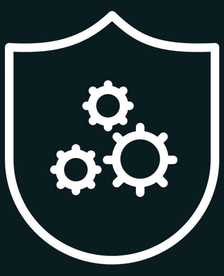
Prevent unauthorized access to your accounts

If a malicious actor were able to gain unauthorized access to your account, they could steal or destroy private data. You can prevent unauthorized access by creating strong and unique passwords. Strong passwords should contain a mixture of upper and lowercase letters, numbers, and symbols. We recommend enabling two-factor authentication as this is an easy way to add an additional layer of security that a cybercriminal must go through before they can access your account.

Strong passwords & 2-factor authentication

4

Be vigilant!



Review privacy settings regularly

Review & use privacy settings when creating an account

Privacy settings are used to control how organizations handle your personal information online. If you use social media, you might have seen privacy settings allowing you to control who can access your profile and what information they can see. If your profile is public this means everyone can view what you post which could pose a risk to your privacy. Before creating a digital account, you should read and understand what data the company will collect about you and what privacy settings you can enable..

Reduce your digital footprint

5

Delete digital accounts you no longer use

Over the years you have probably created lots of digital accounts that you no longer monitor or use. These accounts can contain information that is valuable to a cybercriminal. To keep your data safe, you should remove personal identification details, payment information, and private data or simply delete the old account once it is no longer required.

Old accounts can be a cybercriminal's treasure trove