Identity Theft Protection Kit

Legal Disclaimer

- **No liability for any errors or omissions**

  The information contained in this Handout has been provided by My Protected ID for information purposes only. This information does not constitute legal, professional or commercial advice. While every care has been taken to ensure that the content is useful and accurate, My Protected ID gives no guarantees, undertakings or warranties in this regard, and does not accept any legal liability or responsibility for the content or the accuracy of the information so provided, or, for any loss or damage caused arising directly or indirectly in connection with reliance on the use of such information. Any errors or omissions brought to the attention of My Protected ID will be corrected as soon as possible. The information in this handout may contain technical inaccuracies and typographical errors. The information on this website may be updated from time to time and may at times be out of date. My Protected ID accepts no responsibility for keeping the information in this website up to date or any liability whatsoever for any failure to do so.

- **The material on this handout does not constitute legal and professional advice**

  Any views, opinions, and guidance set out in this handout are being provided for information purposes only. We do not claim to be legal and professional advice or a definitive interpretation of any law. Anyone contemplating an action in respect of matters set out in this handout should obtain advice from a suitably qualified professional adviser based on their unique requirements.

- **No Warranty or Endorsement**

  My Protected ID does not make any warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, nor does it assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, nor does it represent that its use would not infringe privately owned rights. Reference in this handout to any specific commercial service, products, process or service by trade name, copyright, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by My Protected ID. The views and opinions of authors expressed herein do not necessarily state or reflect those of My Protected ID and shall not be used for advertising or product endorsement purposes.

- **No responsibility for other websites**

If you access external websites through a link from the handout of My Protected ID, please note that My Protected ID has no control over the content on external websites. The links to external websites are provided as a matter of convenience only, and should not be taken as an endorsement by My Protected ID of the contents or practices of those external websites, for which My Protected ID assumes no responsibility or liability.

- **Third Party Company and Products**

Any suggestion, reference, indication, or mention to third party companies and, or products on the handout of My Protected ID, is for purely informational purposes only. This information does not constitute either an endorsement or a recommendation. Unless clearly stated otherwise, all third party products and services must be ordered directly from the vendor, and all licenses and warranties take place between you and the vendor. My Protected ID accepts no liability whatsoever for the use or misuse of any third party companies and their products and services.

Online Identity Protection

Over 9 million North Americans have their identities stolen each year, and at least 534 million personal records have been compromised since 2005 through database attacks.

Here are some tips to help you protect your online identity.

1. Install and use robust, up-to-date security software for your computer and smartphone. Update your operating system regularly. Preventing your phone or computer from becoming infected with malicious software is critical. It is generally too late after a breach, as you have already given criminals the key to your online actions.

2. "If it's too good to be true, it's not true" it's probably a scam. Beware of offers for free products, claims you won a contest you did not enter or get-rich-quick schemes. Learn to pick out scams, spam and phishing sites. Some phishing scams can be easily identified. Other phishing attempts in an email, Instant Messaging, on social networking sites, or websites can look very legitimate.
   To ensure you never fall for a phishing scam, don't click on a link that has been sent to you by someone you don't know, looks suspicious or from a third party that you didn't request the information from.

3. Use strong passwords. Weak passwords are an identity criminal's dream. This is especially true if you use the same password everywhere. Passwords should have a minimum of 12 Characters that includes numbers, symbols, capital Letters, and lower-case letters: Use a mix of different types of characters to make the password harder to crack. Ensure your passwords have nothing to do with your personal information (like a pet, birth dates, pet or age). If your accounts are hacked, having multiple passwords for your online accounts will reduce the overall impact. Multiple passwords make it much more difficult for criminals having the ability to gain access to all your private data at once.

4. Freeze your credit. Be aware; criminals use stolen ID's to open new lines of credit. A credit freeze, also known as a security freeze, is a free tool that lets you restrict access to your credit report. A credit freeze makes it more difficult for identity thieves to open new accounts in your name. This is because creditors need to see your credit report before they approve a new account. There are three main credit reporting agencies you can freeze your credit with Equifax, Experian, and TransUnion.

5. Monitor & review all bank data and credit scores. Look for unknown, or suspicious charges on your credit card and bank statements. Also monitor for new loans, credit cards, and suspicious transactions on your account. Take immediate steps to have these terminated and investigated.

6. Be smart with your online purchases. Only use reputable websites. Check search engines for reviews. Research retailers online to make sure they're legitimate. Make sure the website is secure. Dig deep into the site and review. Look for a secure, encrypted connection when asking for your personal and financial information. Look for HTTPS and the lock icon in the address bar of your favorite browser. When making purchases do not use public Wi-Fi. Pay by using a credit card.

7. Understand your default privacy settings on social networking sites. Know how to change them to increase your security preferences.

8. Limit location settings. Limit or disable the location settings on videos and photos you post to social networking sites.

Clues That Someone Has Stolen Your Information

Bank withdrawals that you can't explain.

Missing mail and bills.

Credit approval denied or subjected to high interest rates for no apparent reason.

You are receiving new credit cards sent to you that you did not apply for.

Debt collectors calling about unknown debts

Unusual or unknown accounts or charges on your credit report.

Bills for services you didn’t use.

Your health plan contacts you for issues you know nothing about

Government Revenue Services notifies you that more than one tax return was filed in your name, or that you have income from an employer you don’t work for.

When you receive notice that your information has been compromised by a data breach at a company where you do business or have an account.

How to Protect Yourself from Identity Theft

With millions of people affected by identity theft each year, the below are some steps and strategies you can implement to ensure protection:

Criminals look for the path of least resistance. They look for shortcuts and the easy pickings for committing theft and identity theft crime.

Do Not Publish Your Personal Information

One of the easiest pickings is when the victim publically broadcasts their personal information including address and phone number to the world.

Do not post or publish any of your personal information on items you own (example: keys, luggage, backpack, laptop, smartphone, or any other personal property).

Instead, tag your property with durable recovery tags, and key tags that offer worldwide protection. Attach the tag to identify and protect anything you wish. Make sure the tags do not have your personal information (name, address, phone number, email address) on them. You may wish to use investigative recovery tag services that protect your property. Use a service such as www.SearchAndReturn that conducts a comprehensive investigation after an item goes missing. They also protect your identity because each of their recovery tags has an individual serial number with a 24/7 call center contact information, instead of your name & address.

Check Your Credit Annually

Visit a website such as www.annualcreditreport.com for a free copy of your credit report and verify all information is accurate. For an extra layer of protection, consider enrolling in a credit monitoring service which can monitor all three credit reporting agencies in real time and alert you to any unusual activity.

Review Credit and Debit Card Statements Monthly

Take time to ensure all transactions are legitimate. If you see a questionable charge, contact your bank or credit card company immediately.

Keep Your Personal Information Secure

Don’t share personal information such as your full name, date of birth, Social Security Number, address or phone number over the internet unless it’s a site you’ve initiated contact with and you’re certain it’s secure. Refrain from posting personal details such as your birthday or address on social media sites.

Limit What You Carry

Don’t carry your social security card and limit the number of credit cards you have on hand.

Purchase a Micro-Cut Shredder

This machine ensures that your documents cannot be pieced back together. Use it to turn old financial statements, bills; credit card offers and any other secure or personal information into paper confetti.

Opt-Out

You can opt out of prescreened offers for credit cards, insurance and more by calling 1-888-567-8688 or visiting www.optoutprescreen.com.

Keep Your Passwords Safe, Secure and Unique

Make sure your passwords are strong and get creative with them. Use a combination of letters, numbers, and spaces. Safeguard your computer with firewall, antivirus and spyware protection and update them often. This will protect your computer and files against intrusions.

Be Cautious of What You Click

Be extremely suspicious of emails from strangers. Do not click on them until you double check. Even if you receive an e-mail from a friend with attachments and hyperlinks, be aware that opening them could expose a virus to your computer and files. Take your time, look closely at the email and attachments and determine if any part of the e-mail looks suspicious before clicking on any files or hyperlinks.

Seniors - Common Types of Fraud and Scams

Identity Theft

Identity theft occurs when a criminal steals your personal information to take on your identity. The more detailed the personal information stolen, the more valuable it is to the criminal. Information like your social security number, bank personal identity number (PIN), drivers license, health card, or online password are just a few examples. Losing your wallet, purse, or mail can be a gold mine of opportunity for the identity theft criminal

Once the criminal has your information, they go to work committing their illegal acts like applying for credit cards, loans, making purchases, or withdrawing bank funds.

Credit and Debit Card Fraud

Credit card and debit card fraud take place when a criminal uses your card, or the card information and makes purchases or withdraws money from your account. Prevention tips include ensuring your card is always in sight, memorizing your PIN, and shielding others from watching you enter your PIN.

Online Scams

“If it’s too good to be true, it’s not true” it’s probably a scam. Beware of offers for free products, claims you won a contest you did not enter or get-rich-quick schemes. One of the more successful scams against seniors is receiving a phone call or message stating there is a problem with their income tax or bank account.

Learn to pick out scams, spam and phishing sites. Some phishing scams can be easily identified. Other phishing attempts in an email, Instant Messaging, on social networking sites, or websites can look very legitimate. Look for spelling and other mistakes, including grammar. However, some scams look like they are coming from somebody you know. They may ask you to click on a link or provide your password or other personal, or financial information. It is strongly suggested that you do not follow through with the request and instead contact that person to verify.

To ensure you never fall for a phishing scam, don’t click on a link that has been sent to you by someone you don’t know, looks suspicious or from a third party that you didn’t request any information from.

Door-to-Door and Phone Scams

Be aware – the scam can be very detailed and seemingly legitimate. Criminals will go to great lengths to acquire background information on you in advance of the scam. They may

have already gathered some personal information about you - this is called social engineering.

The criminal will either call or come to your door pretending to be a representative of a charitable organization, an employee of IRS (or even law enforcement), or a long lost relative. It may be high pressured with threats of severe consequences, or they might offer you a free prize or trip. Do not feel pressured and don't give the person any information or money.

Tips and Safeguards

If possible, keep all personal documents in a secure place. Unless needed, don't carry your birth certificate, passport or social security card with you.

Never give or tell another person your account passwords or PIN. Cover your hand when entering your PIN when making transactions at stores or bank machines.

Shred old banks statements, bills and other documents that have your personal information on them.

Do not click on links, open attachments or respond to e-mails sent by people you do not know. Pay attention to e-mails from your bank. They will not send you anything by e-mail unless you request it.

Do not give out your banking information, credit card, or personal information to someone over the internet, over the phone, or at the door unless you know them.

Watch out for offers that are "time-limited" Do not sign a contract or agreement. Instead, take some time, talk to others and think it over.

If you have advertised an item for sale online, beware of fake buyers. They offer to send you the money in advance. Usually, the amount the fake buyer is willing to send to you is more than your asking price. Here are some tips to protect yourself.
https://www.kijiji.ca/kijijicentral/general/how-to-recognize-fraud-fake-buyers/

Before hiring someone or agreeing to have work done on your home, ask for proof of identity and references and check them.

When in doubt, use internet search engines to research the potential scam. Look for trusted and verified reviews and postings.

Protect Your Kids Identity Online

Protect your digital identity and information – your digital identity is like your fingerprint or DNA. You must always be thinking about protecting yourself. Think about the information that is being requested and collected from you. Also, think about who is collecting this information and where it is being stored.

Use Strong Passwords – Protect your password and remember to use a robust password that is exclusive to every individual and website. If possible, do not write down your password or share with others you do not trust. Many electronic and online tools exist to help you manage and store your passwords.

Do not post anonymously – avoid smartphone apps and websites that allow anonymous postings. Devices should be in plain view and public areas. They should not be in the bedrooms. With youth, it is important to discuss and set limits and boundaries on acceptable device use. It is also important to monitor social media websites.

Social etiquette – simple put…think before you post. Consider both yourself and others before you post. If you are unsure of your potential post – hold back from posting. Wait 24 hours and reassess. If you would not say it in a public setting, do not post it online. Think about the lasting consequences around posting offensive comments, photographs and shared locations on social media.

Student safety – device theft, robbery and other violent crimes within and outside the school is growing concern. Not only does this place the student at a higher risk, but school districts also run the possibility of having a shortfall of devices allocated for learning.

Students must learn and practice theft prevention techniques that include (1) password protect the device (2) keeping their device out of sight when in public – do not advertise you have an expensive smartphone or tablet (3) if ever confronted by thieves wanting to steal their device, give it up immediately and run the other way (4) when authorized or applicable, enable device location features (5) do not leave your device unattended, especially in public locations.

<u>Things to Think About</u>

<u>Now:</u>

Would I say this in real life?

Am I hurting anyone else by posting this?

Will I regret this later?

Have I reviewed all the pictures carefully?

It is necessary to share this with ‘the world?’

Would my parents, coaches and or teachers approve of this post?

And in the future:

Could this post have any negative effect on me pursuing future employment?

If I have a family, would I want my children seeing this?

Could what I am posting bring legal ramifications against me later?

Would my chosen College or University still consider my application after seeing this post; would their team coach?

CONSIDER ALL POSTS TO BE PERMANENT!

DIGITAL CITIZENSHIP

1. **Digital Access**
2. **Digital Commerce**
3. **Digital Communication**
4. **Digital Literacy**
5. **Digital Etiquette**
6. **Digital Law**
7. **Digital Rights & Responsibilities**
8. **Digital Health & Wellness**
9. **Digital Security**

1. **Digital Access – Full electronic participation in society**

Digital access is an important concept of digital citizenship. Digital access pertains to the fair accessibility to technology as well as the ability to use it to enhance the learning process for all involved. Digital access is an equitable opportunity for the same education for every student via the use of technology.

2. **Digital Commerce – Electronic buying and selling of goods**

Digital commerce is the buying and selling of goods and services using the Internet, mobile networks and commerce infrastructure.

This includes both legal and illegal forms of commerce and buyers need to be aware of the risks of making online purchases.

3. **Digital Communication – Electronic exchange of information**

In today's society, everyone has the opportunity to communicate and collaborate with anyone from anywhere and anytime. Unfortunately, many users make poor decisions when faced with so many different and constant digital communication options. Concerns include texting and driving, device addition, cyberbullying, etc.

4. **Digital Literacy – the process of teaching and learning about the use of technology**

Digital literacy refers to how a person utilizes technology to interact with the world around them**.**

5. **Digital Etiquette – electronic standards of conduct or procedure**

Digital etiquette is based on a set of rules to make the internet better for you and others. Digital etiquette is about treating people with respect and courtesy and respect online.

6. **Digital Law – electronic responsibility for actions and deeds**

Digital Law is the electronic responsibility for deeds and actions either ethical or unethical. The digital law refers to the ethics within technology. Unethical use of technology exhibits itself in the form of theft and crime.

7. **Digital Rights and Responsibilities – those freedoms extended to everyone in a digital world**

The definition of digital rights and responsibilities has the right and freedom to use all types of digital technology while using technology acceptably and appropriately. Users also have the right to privacy and the freedom of personal expression.

8. **Digital Health and Wellness – physical and psychological well-being in a digital technology world**

Digital Health and Wellness concentrates on the use of technology safely and appropriately. In today's technological world, our children are becoming dependent on the use of the internet. It is becoming necessary to inform them about the dangers involved with frequent internet use.

9. **Digital Security – electronic precautions to guarantee safety and self-protection.**

Digital security focuses on teaching our children and students strategies to stay safe in the digital world.

If Its Too Good To Be True, It's Not True

Always start by treating everything as the worst case scenario. Expect something to go "sideways" on you.

A pretty bold statement. But this is one of those life principles that you may want to pay attention to.

You see the world is full of scams, hype, and tricks. We've seen many of them, and there are many more being schemed up daily by a multitude of interesting characters. These scams come in all shapes and sizes, and some of them just seem "so sweet." These scams are so tempting and seem so real and legitimate.

The problem is you want to believe it because you figure your "ship has come in."

Here is our rule of thumb: "If you play with fire, you're going to get burned."

Trust nothing on its face value. Yes, this is sad to say, but all you are doing is investigating deeper by taking this approach. Again, good deals are usually only good for the "other guy."

So our message is simple but powerful: nobody gives something away for nothing or a loss. There has to be a reason why you are getting a deal. You need to ask yourself, why me? Why am I getting this unbelievable deal? Chances are, you're not getting any deal. Most probably you are getting ripped, tricked scammed or at the very least, taking a Big Risk.

At the FutureCents, we believe if you practice our principle, you can greatly minimize your risk exposure to any type of scam or fraud.

So what do you do? Easy!

1) Trust nothing. If It's Too Good To Be True. It's not True.

You can't go wrong with this approach. And if you are wrong, well you have practiced a principle that will serve you well the next time (and there will be a next time).

2) Take your time. Guaranteed there is going to be a sense of urgency on the deal. You name it; they will try everything they can to pressure you into it. Or, you will put that false sense of urgency on yourself by not wanting to lose the deal. It is very tough to say >>>Slow Down<<<, but much smarter in the long run because you catch your breath and look at the situation with fresh eyes.

3) It is easy to Say No. Let Me Investigate This and Get Back to You.

Now you have control. Check out the deal more thoroughly when you have time. Talk to others.

Remember, the pressure is the name of their game. You control the situation, not them.

4) Finally, just ask yourself, what am I prepared to accept as a loss? In other words, expect you are going to get ripped and decide if the loss, the risk is acceptable to you. If you're not prepared, don't do it.

We believe in the principle of treating everything at first as the "worst-case scenario." After you determine the situation is not as bad; you can always relax your position.

Again, a little proactive precaution can save you a major headache down the road.

Identity Theft Recovery Check List

Contact your local police force and file a report. Bring your government issued ID, proof of address and all other relevant information. Ask for a copy of the police report.

Contact your bank/financial institution and credit card company. Speak to the fraud department. Explain that someone stole your identity. Have them close or freeze the accounts.

Change logins, passwords, and PINs for your accounts.

Reporting Identity Theft

United States of America

Place the three national credit bureaus and place a free fraud alert on your credit reports.

www.Experian.com/fraudalert 1-888-397-3742
www.TransUnion.com/fraud 1-800-680-7289
www.Equifax.com/CreditReportAssistance 1-888-766-0008

A fraud alert is free. It will make it harder for someone to open new accounts in your name. You will receive a letter from each credit bureau. It will confirm that they placed a fraud alert on your file.

Obtain your free credit reports from Equifax, Experian, and TransUnion. Go to www.annualcreditreport.com or call 1-877-322-8228.

Report identity theft to the FTC. www.IdentityTheft.gov or call 1-877-438-4338. Include as many details as possible. IdentityTheft.gov will create your Identity Theft Report and recovery plan.

More information is available at https://www.usa.gov/identity-theft

Canada

Contact the two national credit bureaus and place a fraud alert on your credit reports.

Equifax Canada Toll-free: 1-800-465-7166

TransUnion Canada Toll-free: 1-877-525-3823

Report identity theft and fraud. Contact the Canadian Anti-Fraud Centre

More information is available at http://www.rcmp-grc.gc.ca/scams-fraudes/id-theft-vol-eng.htm