# Electric Scotland's Weekly Newsletter for August 2nd, 2019

For the latest news from Scotland see our ScotNews feed at:
https://electricscotland.com/scotnews.htm

## Electric Scotland News

I added a book of Gaelic stories this week in the Gaelic language so of course if you can't speak Gaelic you won't be able to read them. That said I do like to try and do my bit to help preserve the Gaelic language and as I can't speak it either I'm also hoping someone out there might help by translating some of them for us.

The book can be found on our Gaelic page at: https://electricscotland.com/gaelic/ and it's called "The Highlanders' Friend".

You might like to check this page as I do have two very good Gaelic videos on that page. The first one is teaching you how to sing a Gaelic nursery rhyme which is apparently sung to a wee boy and if anyone can translate the Gaelic into English I'd appreciate you sending in a translation.

The other is a documentary on Gaelic in Nova Scotia with a mix of Gaelic and English. I just watched it again and enjoyed it and must confess I hadn't recognised that some of it is actually in spoken English.

---

You can view a video introduction to this newsletter at:

https://youtu.be/VOc8PwPY2h0

### Scottish News from this weeks newspapers

Note that this is a selection and more can be read in our ScotNews feed on our index page where we list news from the past 1-2 weeks. I am partly doing this to build an archive of modern news from and about Scotland as all the newsletters are archived and also indexed on Google and other search engines. I might also add that in newspapers such as the Guardian, Scotsman, Courier, etc. you will find many comments which can be just as interesting as the news story itself and of course you can also add your own comments if you wish.

### Funding model should be made clearer, say MPs

The method by which Scottish government funding is calculated should be made more transparent, a Westminster committee has recommended.

Read more at:
https://www.bbc.com/news/uk-scotland-scotland-politics-49111484

### A more prosperous UK outside the EU

One of the important wins will be to resume our full voting membership of the World Trade Organisation.

Read more at:
http://johnredwoodsdiary.com/2019/07/26/a-more-prosperous-uk-outside-the-eu/

### Boris Johnson is off to a flying start after crushing Jeremy Corbyn in the first meeting in Parliament

THE glum faces of Labour MPs revealed it all as Boris Johnson went head-to-head with Jeremy Corbyn for the first time and crushed him underfoot.

Read more at:

https://www.thesun.co.uk/news/9587658/boris-johnson-jeremy-corbyn-first-meeting-parliament/

### Alister Jack: What do we know about the new Scottish Secretary?

Alister Jack is a relative newcomer to Westminster, having been first elected in the 2017 snap election.

Read more at:
https://www.bbc.com/news/uk-scotland-scotland-politics-49103859

### How should the UK change its foreign policy once out of the EU?

Once we are out of the EU the UK regains its vote and voice in world bodies.

Read more at:
http://johnredwoodsdiary.com/2019/07/27/how-should-the-uk-change-its-foreign-policy-once-out-of-the-eu/

### In pictures: Langholm Common Riding

Langholm has held its annual common riding event around the borders of the Dumfries and Galloway town.

View the pictures at:
https://www.bbc.com/news/uk-scotland-south-scotland-49143464

### Why a US-UK trade deal ought to mean us finally getting some sense from Brussels

Prime Minister Boris Johnson has already made it clear he will urgently look for a trade deal with President Trump.

Read more at:
https://brexitcentral.com/why-a-us-uk-trade-deal-ought-to-mean-us-finally-getting-some-sense-from-brussels/

### What I learnt from Canada about legalising cannabis

Despite legalisation, many Canadians still buy cannabis on the black market

Read more at:
https://capx.co/what-i-learnt-from-canada-about-legalising-cannabis/

### Let's transform UK agriculture

All the time we have been in the EU the Common Agriculture Policy has kept the UK under controls which have not suited us.

Read more at:
http://johnredwoodsdiary.com/2019/07/30/lets-transform-uk-agriculture/

### The London Stock Exchange is turning away from Europe and endorsing Global Britain

The LSE's latest deal is a huge vote of confidence in London as a financial centre

Read more at:
https://capx.co/the-london-stock-exchange-is-turning-away-from-europe-and-endorsing-global-britain/

### Brexit 'opportunity to correct farm funding failings

MPs on Westminster's Scottish Affairs Committee said leaving the EU presented a chance to address failings in the current formula.

Read more at:
https://www.bbc.com/news/uk-scotland-49168341

### Education experts say children are reaping the benefits of boom in early-learning centres held in countryside and parks

In the past 10 years, Scotland has experienced a boom in outdoor nurseries, which see children aged three and up spend the majority or all of the day learning in the countryside and parks.

Read more at:
https://www.sundaypost.com/fp/education-experts-say-children-reaping-the-benefits-of-boom-in-early-learning-centres-held-in-countryside-and-parksruaridhs-storyits-lovely-to-hear-him-come-home-and-ta/

### The Irish backstop is a shameless threat to the UK's integrity - it must be ditched

It's extraordinary that rejecting the partition of the UK is portrayed as hardline

Read more at:
https://capx.co/the-irish-backstop-is-a-shameless-threat-to-the-uks-integrity-it-must-be-ditched

### Johnson has the inestimable advantage of a divided Opposition

The best news yesterday for Boris Johnson was written by Tony Blair's former Director of Communications.

Read more at:
https://www.conservativehome.com/thetorydiary/2019/07/johnson-has-the-inestimable-advantage-of-a-divided-opposition.html

### The Asian Century Is Over

Beset by conflicts, stagnating economies, and political troubles, the region no longer looks set to rule the world.

Read more at:
https://foreignpolicy.com/2019/07/31/the-asian-century-is-over

## Electric Canadian

### The Canadian Horticulturist

Volume 36 (1913) can be read at:
https://www.electriccanadian.com/transport/agriculture/Horticulturirst.htm

### Canadian Poets

Chosen and Edited by John W. Garvin, B.A. (1916) (pdf)

A biography and examples of their poems and this can be read at:
https://www.electriccanadian.com/lifestyle/canadianpoets.pdf

### Oatmeal and the catechism:

Scottish Gaelic settlers in Quebec by Margaret Bennett (1998). This book can be borrowed from the Internet Archive at: https://archive.org/details/oatmealcatechism0000benn

### Five Years Development of Machine Tools in Canada

By G. C. Keith BSc. (pdf)

You can read this at: https://www.electriccanadian.com/transport/industrial/canadianmachiner06.pdf

### Canadian Railroader

The circulation of the magazine is devoted to the Canadian Railroad Men Volume 1 (1917)

You can read Volume 1 at:
https://www.electriccanadian.com/magazines/canadian-railroader-quarterly_v1-no1.pdf

### Montreal Origins

Nicole O'Bomsawin, of the Abenaki First Nation, shares some of the history of the First Nations that have been established in the Montreal area for centuries. English sub titles are available in this film which can be viewed at: https://www.canadashistory.ca/explore/first-nations-inuit-metis/montreal-chronicles-origins

### Canadian Magazine

I found Volume 1 of the Canadian Magazine and while a little out of focus was able to ocr in the introduction to the publication which you can read on our Magazines page at:
https://www.electriccanadian.com/magazines/index.htm

## Electric Scotland

### Scottish Eccentrics

By Hugh MacDiarmid

The distinguished Scottish poet and literary critic who writes this book recalls how Bernard Shaw in On The Rocks ironically declares that the massacres after the Battle of Culloden were not "murder" but simply "liquidation," since the slain Scots in question were "incompatible with British civilization." He then surveys the whole field of Scottish biography, and shows how true this has proved of an amazing number of distinguished Scots, no matter how successfully the bulk of the Scottish people have been assimilated to

English standards since the Union. The facts are irresistible and bring out the "eccentricity" of Scottish genius in an extraordinary fashion.

The author gives full-length studies often outstanding Scottish eccentrics, including Lord George Gordon of the "Gordon Riots"; Sir Thomas Urquhart, the translator of 'Rabelais', "Christopher North"; "Ossian" (James Macpherson, M.P.); James Hogg, the Ettrick Shepherd; and William McGonagall, perhaps the world's best "bad poet". But he supports these leading cases with apt material drawn from the lives of hundreds of Scots of every period in history and every walk of life, and in this way builds up a brilliant panoramic picture of Scottish psychology through the ages, singularly at variance with all generally accepted views of the national character.

You can read this book at: https://electricscotland.com/lifestyle/eccentrics.htm

### Discovering Scotland
by Reader's Digest

This video is 1hr 46min playing time and can be viewed at: https://archive.org/details/DiscoveringScotland

### Harry Gordon
Entertainer

Stan Bruce made me aware of this person and send me some info on him which I've been able to add a sound clip and picture. You can see this at: https://electricscotland.com/poetry/harrygordon.htm

### Beth's Newfangled Family Tree
Got in section 1 of the August 2019 edition.

You can read this at: https://electricscotland.com/bnft/index.htm

### Hylton Newsletter
This newsletter covers his trip to Iceland and you can read this at:
https://electricscotland.com/familytree/newsletters/hylton/newsletter2019Iceland.pdf

### Massacre of Christians in Syria
Added this article from Good Words published in 1860.

You can read this at: https://electricscotland.com/history/goodwords/goodwords233.htm

### The Lord's Prayer
Another article from Good Words in 1860 which you can read at:
https://electricscotland.com/history/goodwords/goodwords234.htm

### The Highlands of Scotland in 1750
From Manuscript 104 in the King's Library, British Museum with an Introduction by Andrew Lang (pdf)

A lot of clan information as the authors tour was to detail the conditions in Scotland for the King. You can read this at: https://electricscotland.com/history/highlandsscotland1750.pdf

### Scottish Society of Louisville
Got in the August 2019 newsletter which you can read at:
https://electricscotland.com/familytree/newsletters/Louisville/index.htm

### The Highlanders' Friend
Second Series, A Further Selection from the Writings of the Late Very Reverend Norman MacLeod, D.D. (1901) (pdf). This book is in the Gaelic language and you can read it at:
https://electricscotland.com/gaelic/highlandersfriend.pdf

## The Story

As this is an ongoing issue with anyone that uses the Internet I thought I'd bring you this detailed article from the Malawarebytes folk....

### Identity Theft

Identity theft occurs when a criminal obtains or uses the personal information; e.g. name, login, Social Security number, date of birth, etc., of someone else to assume their identity or access their accounts for the purpose of committing fraud, receiving benefits, or gaining financially in some way.

What is identity theft?
We're all in the middle of an identity crisis—an identity theft crisis, that is.

According to a 2017 report from Javelin Strategy, there were 16.7 million victims of identity theft in the United States, while total losses across all types of identity theft reached $16.8 billion. For perspective, if the criminals responsible banded together to create their own country, which we'll call Crimeland (Crimea is already taken), the nominal gross domestic product would put Crimeland at 118th place just below Gabon and above Georgia.

The top forms of identity theft according to the Federal Trade Commission (FTC) Data Book 2018 are:

Credit card
Tax
Phone or utilities
Bank
Loan or lease
Government documents and benefits
Other (a catchall for medical, social media, and other less common forms)

Identity theft occurs when a criminal obtains or uses the personal information; e.g., name, login, Social Security number (SSN), date of birth, etc., of someone else to assume their identity or access their accounts for the purpose of committing fraud, receiving benefits, or gaining financially in some way.

In the US, “identity theft” wasn't legally defined until 1998. It was then Congress passed the Identity Theft and Assumption Deterrence Act, which made identity theft a prosecutable offense in and of itself. Prior to this, identity theft was prosecuted under a hodgepodge of state and federal fraud statutes designed with old-timey grifters and con-artists in mind (think Leonardo DiCaprio in the 2002 film Catch Me if You Can).

International laws vary from one country to the next. Of note, EU citizens are protected under the General Data Protection Regulation (GDPR). The UK followed suit with the Data Protection Act 2018.

Pre-Internet criminals typically had to go through your physical mail box or suffer the indignity of rummaging through your smelly trash to get the information they needed to steal your identity—like those “you're already approved,” pre-screened credit offers we all get in the mail.

Thanks to the miracle of modern technology, today's cybercriminals don't have to work nearly as hard to invade your privacy, but they stand to gain so much more. Big businesses and the large caches of data contained on their networks present a much more lucrative target than piecemeal attacks on individual consumers. Accordingly, attacks on businesses are up 235 percent year over year, according to the Malwarebytes Labs Cybercrime Tactics and Techniques report. At the same time, attacks on consumers went down almost 40 percent.

According to the Identity Theft Resource Center's (ITRC) 2018 End-of-Year Data Breach Report there were 1,244 data breaches, exposing over 446 million records in 2018.

Chances are your data has already been compromised in a data breach.

For example, the 2013 Yahoo data breach affected all three billion Yahoo user accounts (yes, that's billion with a “b”). If at any point in time you had an account with Yahoo, you're a victim. The stolen data included names, emails, a mix of encrypted and unencrypted passwords, and security questions and answers—all of which are immensely useful for hacking into other accounts that use the same login credentials (aka credential stuffing attacks).

As a result of the Yahoo data breach and others like this, this, and these, your personal data is likely for sale right now on the Dark Web. The Dark Web is like the Bizarro World version of the Web we use every day. While the average person uses the normal Web to stream movies, buy groceries, and download software. The Dark Web caters to a different kind of customer looking for illegal porn, drugs, and caches of stolen data.

According to the New York Times, three shady buyers paid $300,000 each on a Dark Web marketplace for the stolen Yahoo data.

Collection 1, the largest assemblage of stolen data in history was at one point selling on the Dark Web for a mere $45.

This is a familiar narrative within the world of cybercrime—you place your trust in an organization, organization is hacked, your data is stolen, cybercriminals sell your data on the Dark Web, buyers use your data to commit fraud.

Before you resign yourself to victimhood, take heart. There are steps you can take to safeguard the privacy of your data and protect your identity from would-be identity thieves. Even if the bad guys already have your personal information, you can make your information entirely useless to them.

Let's take a deeper dive into the sordid world of identity theft, the signs, the causes, how to protect yourself, and what to do if your identity has already been stolen.

What are the signs of identity theft?

You stop receiving your regular bills and credit card statements.
You receive statements for accounts you never opened.
Debt collectors start calling you day and night about debts you've never heard of.
The IRS alleges you failed to report income for a company you never worked for.
You see withdrawals/charges on your bank or credit card statement that you didn't make.
You try to file your taxes only to discover that someone else beat you to it.
You try to file your taxes and find someone claimed your child as a dependent already.
Your credit report includes lines of credit you never opened.
Your credit score fluctuates wildly and for no apparent reason.
The most obvious sign—you receive a notification that you've been the victim of a data breach.

What are the types of identity theft?

Credit identity theft happens when a scammer steals your credit card number outright and uses it to make fraudulent purchases or obtains a credit card or loan under your name. According to the FTC, credit card related identity theft was the most common form of ID theft for 2018—up 24 percent over the previous year.

Tax identity theft occurs when a scammer gets a hold of your SSN and uses it to obtain a tax refund or get a job. This might come as a result of a data breach that exposes your SSN online, for example. The US Internal Revenue Service doesn't get much love from taxpayers, but the organization's efforts to reduce tax-related identity theft appear to be working. The IRS reports cases of tax-related identity theft are down 38 percent from 401,000 in 2016 to 242,000 in 2017.

Child identity theft. Why would someone want to pretend to be a child? Many reasons.
Scammers can use your child's SSN to obtain a tax refund, claim them as a dependent, open a line of credit, get a job, or obtain government ID. There are lots of ways you can protect against child identity theft, including freezing your kid's credit. Generally, they need to be under 15 or 16 years of age, though the age limit varies by state (more on credit freezes later).

Medical identity theft happens when criminals use your identity to see a doctor, get medical treatment, or obtain prescription drugs. In years past, medical identity theft could affect your ability to get health coverage or cause you to pay more for treatment. That's not the case anymore thanks to recent changes in the law, but past due medical debts incurred by a scammer can appear on your credit file and hurt your credit score. Seniors are a prime target for medical ID scams, because they receive Medicare and no one will think twice about frequent medical visits. With the Baby Boomer generation entering Medicare age (65+), scammers have more targets than ever before. Medical ID theft is up 103 percent year over year, according to the FTC.

Criminal identity theft happens when a criminal is arrested and provides law enforcement with a name, date of birth, and fraudulent ID based on a stolen identity. Criminal ID theft typically comes up when applying for a job or an apartment. If the employer or landlord performs a background check, the crimes of your nefarious doppelganger might stop you from getting that job or housing.

How does identity theft happen?
Here's a sampling of the more common attack methods cybercriminals use to breach an organization, network, or your personal computer in order to steal your personal information and your identity. And if you're interested in the history of data breaches, head over to our article on the subject.

An exploit is a type of attack that takes advantage of software bugs or vulnerabilities, which cybercriminals use to gain unauthorized access to a system and the data contained within. These vulnerabilities lie hidden within the code of the system and it's a race between the criminals and the cybersecurity researchers to see who can find them first. The criminals, on one hand, want to abuse the exploits while the researchers, conversely, want to report the exploits to the software manufacturers so the bugs can be patched. Commonly exploited software includes the operating system, Internet browsers, Adobe applications, and Microsoft Office applications.

Spyware and keyloggers are a type of malware that infects your computer or network and steals information about you, your Internet usage, and any other valuable data it can get its hands on; e.g. your usernames, passwords, and SSN. You might install spyware as part of some seemingly benign download (aka bundleware). Alternatively, spyware can make its way onto your computer as a secondary infection via a Trojan like Emotet. As reported on the Malwarebytes Labs blog, Emotet, TrickBot, and other banking Trojans have found new life as delivery tools for spyware and other types of malware. Once your system is infected, the spyware or keylogger sends all your personal data back to the command and control (C&C) servers run by the cybercriminals.

Phishing attacks work by getting us to share sensitive information like our usernames and passwords, often employing social engineering tricks to manipulate our emotions, such as greed and fear. A typical phishing attack will start with an email spoofed, or faked, to look like it's coming from a company you do business with or a trusted coworker. This email will contain urgent or demanding language and require some sort of action, like verifying payments or purchases you never made. Clicking the supplied link will direct you to a malicious login page designed to capture your username and password. If you don't have multi-factor authentication (MFA) enabled, the cybercriminals will have everything they need to hack into your account. While emails are the most common form of phishing attack, SMS text messages (aka smishing) and social media messaging systems are also popular with scammers.

Oversharing on social media. It's not our fault when a social media site like Facebook or Google+ gets hacked, but oversharing personal information on social media does increase our risk of identity theft in the event of a data breach. A Facebook bug allowed spammers to get around login requirements and access personal information for 30 million users. Likewise, a bug in Google+ gave third-party app developers access to personal information, including name, email, DOB, gender, places lived, and occupation for nearly half a million users. Two months later Google pulled the plug on the social media service when it was discovered another Google+ bug exposed over 50 million users. Should you limit your exposure and delete yourself from social media? If you answered yes, check out our guide.

Scam calls and robocalls are live or pre-recorded phone calls designed to trick you out of your personal information. A recent robocall covered on the Malwarebytes Labs blog involved scammers purporting to be from the Social Security Administration. Recipients were accused of “leaving behind trails of suspicious information” and if the recipients do not call the scammers back and confirm their SSN, a warrant would be put out for their arrest. The really grifty part of this scam is that the perpetrators used spoofing technology to make the calls appear to come from the Social Security Administration's national customers service number. According to the FTC, scam calls from people pretending to be from the Social Security Administration went up 994 percent from 3,200 in 2017 to 35,000 in 2018.

A SQL injection (SQLI) is a type of attack that exploits weaknesses in the SQL database management software of unsecure websites in order to get the website to spit out information from the database. Malwarebytes Labs ranked SQLI as number three in the The Top 5 Dumbest Cyber Threats that Work Anyway. A bad guy enters malicious code into the search field of a retail site, for example, where customers normally enter searches for whatever they're trying to buy. Instead of returning with a list of search results, the website will give the hacker a list of customers and their credit card numbers. This may sound like an oversimplification, but it really is this easy. Attackers can even use automated programs to carry out the attack for them. All they have to do is input the URL of the target site then sit back and relax while the software does the rest.

Broken or misconfigured access controls can make private parts of a given website public when they're not supposed to be. For example, a website administrator at an online retail site will make certain folders on the network private. However, the web admin might forget to make the related sub-folders private as well, exposing any information contained within. While these sub-folders might not be readily apparent to the average user, a cybercriminal with strong Google-fu skills could find those misconfigured folders and steal the data inside.

Credential stuffing. In the aftermath of a data breach, affected organizations will often force reset the passwords for all impacted users, but that doesn't necessarily mean everyone is safe. Cybercriminals can use stolen emails, usernames, passwords, and security questions/answers to break into other accounts and services that share the same information. Using off-the-shelf automation tools designed for testing webpages, cybercriminals enter a list of stolen usernames and passwords into a website until they land on the right credentials for the right website. This is credential stuffing and while it can be used to hack individual consumer accounts, it's typically used as part of a remote desktop protocol (RDP) attack.

Should I sign up for credit monitoring?
After a data breach, affected companies will usually offer free credit and identity monitoring services as a conciliatory measure. Are these monitoring and protection services actually worth the money?

The Internet consensus seems to be that you shouldn't pay for credit monitoring services, but if it's offered to you for free (i.e., after a data breach) go ahead and sign up.

Writing for the Malwarebytes Labs blog, cybersecurity researcher William Tsing said, “Identity theft monitoring services sound great on the surface. They're not that expensive and seem to provide peace of mind against an avalanche of ever-more damaging breaches. But they don't, at present, protect against the worst impacts of identity theft—the theft itself.”

What does “credit monitoring” or “identity theft protection” actually entail and why does everyone seem to think these services stink?

As Tsing pointed out, the biggest problem with credit monitoring services is that they can't actually stop cybercriminals from stealing your identity. Though they can alert you when someone opens up a line of credit under your name. Think about it this way, these services alert you to changes on your credit report if you can't be bothered to check your own credit report. If that's the case, then you may want to consider signing up and paying someone else to monitor your credit file for you, but the bottom line is that these credit monitoring services are just that—monitoring services, not protection.

How can I protect myself from identity theft?
If all of this talk about identity theft and data breaches upsets you, you're in good company. A data privacy survey conducted by Malwarebytes Labs found the majority of respondents want to take steps to protect their data online and distrust search engines and social media with their data.

As we've established, you probably don't need to pay for identity theft protection services that don't actually protect you against anything. Instead, follow our completely free, DIY tips below.

Claim your three free credit reports. Everyone should get in the habit of checking their credit file regularly. Every consumer gets one free credit report from each of the three major credit bureaus (Equifax, Experian, and TransUnion) at annualcreditreport.com. You don't have to take them all at once—nor should you. By spreading your free reports over the course of a year, you can check your credit file three times a year, on your own, without paying a dime to the so-called “credit monitoring” services.

Put a free freeze on your credit file. As of 2018, credit freezes are free for everyone, no matter what state or country you live in. With a freeze in place, no one (including you) can look at your credit file, let alone open a line of credit. As long as you don't anticipate applying for a loan or a credit card anytime soon this is a great option. In the event that you need to open a line of credit, you can contact the credit bureaus and stop the freeze at any time with the PIN you received when you froze your account. The only hassle is that you must contact each credit bureau individually to enact or remove a freeze. You should submit a freeze for your children while you're at it. Yes, the credit bureaus maintain credit files for your underage children. Unlike an adult credit freeze, where you might have to turn it on and off over time to buy car or apply for a loan, you can freeze your kid's credit and forget about it until they turn 18.

Opt-out of pre-screened credit offers. If you have good to excellent credit, you likely receive several credit card offers in the mail every week. Pre-screened offers don't hurt your credit score and they often include big sign up bonuses, but they also leave you exposed to credit card fraud. Criminals can steal these offers out of your mailbox and open a credit account under your name. It's a decidedly low-tech form of identity theft, but it works. You can limit your exposure by visiting optoutprescreen.com and opt-out of pre-screened credit cards. This stops the credit bureaus from sharing your credit file with creditors and insurers. Plus, you'll be saving some trees and reducing the glut of junk mail that fills your mailbox every month.

File your taxes early. The IRS will only accept one tax return per SSN. Beat scammers to the punch and file your taxes before they can do it for you.

Get an identity protection PIN from the IRS. If you're willing to jump through an extra hoop when tax season comes around, consider obtaining an identity protection PIN. Anyone who tries to file a tax return using your SSN, including you and your accountant, will need to provide the special number assigned to you by the IRS. The number changes every year and can be obtained online or sent to you in the mail.

Watch out for IRS scam calls and phishing emails. The IRS will generally send several notices via snail mail before trying to call or email you. If you receive a threatening call from the IRS demanding immediate payment of back taxes or else, you should hang up, because it's probably a scam. Similarly, be wary of any emails purporting to be from the IRS, and definitely don't click any links or open any attachments. Keep in mind, the IRS will never demand immediate payment without a chance to appeal, arrest you (unless you're committing tax fraud or evasion), or demand payment using weird methods like wire transfer or iTunes gift cards. Moreover, taxes owed are always payable to the US Treasury—without exception.

Use good cybersecurity. As we covered earlier, identity theft often starts with some sort of malware. Granted, there's not much we can do when some business loses our information in a data breach. We are, on the other hand, empowered to stop cybercriminals from attacking us personally by adopting some form of cybersecurity. Malwarebytes, for instance, has the goods for Windows, Mac, Android, iOS and Chromebook. Malwarebytes blocks malware like keyloggers, spyware, and Trojans from getting on your computer or opening up a backdoor and stealing your data. For iPhone fans, Malwarebytes for iOS screens out phone scams and robocalls.

For readers in the UK. First, consider opting out of the open electoral register—it won't hurt your credit score. Second, consider getting a Royal Mail PO box. Both will make it much harder for criminals to get their hands on your personal info by taking your name and address of those huge public lists. And UK readers should still check their credit reports with the three UK bureaus, but keep in mind, you don't get the free annual reports like US consumers.

What do I do when my identity is stolen?
You did everything right. You took every measure possible to keep and protect your identity and then the worst thing happens. You start receiving calls from debt collectors for accounts you never opened, and you see delinquent lines of credit on your credit report.

Here's our identity theft response checklist. Print it out and stick it to your fridge or save it to your desktop as a sobering reminder that identity theft has become a sad fact of life.

Clean up your computer. It may not be immediately obvious how your identity was stolen (e.g., malware, scam call, data breach, etc.) so you may want to take a scorched earth approach to the recovery process. Start with a good cybersecurity program and scan your system for any potential threats. The free versions of Malwarebytes for Mac and Malwarebytes for Windows are a good place to start. Both use advanced detection technology to root out hidden threats on your system.

Reset your passwords for compromised accounts and any other accounts sharing the same passwords. Really though, you shouldn't reuse passwords across sites. Granted, remembering a unique alphanumeric password for all of your online accounts and services is impossible. Consider using a password manager like 1Password. Password managers have the added benefit of alerting you when you land on a spoofed website. While that login page for Google or Facebook might look real, your password manager won't recognize the URL and won't fill in your username and password for you.

File an identity theft report with the FTC. Some businesses and organizations require an FTC identity theft report as the first step towards documenting your identity theft. You'll also need the report to obtain an extended seven-year fraud alert from the credit bureaus and to remove fraudulent accounts from your credit file. Fun fact—the FTC is a federal law enforcement agency. This means you don't have to file another report with your local law enforcement agency, unless you know the identity thief personally or your creditors demand it as proof that you're the victim.

Contact your bank and creditors. You can be liable for some or all fraudulent charges and stolen funds if you don't report lost or stolen debit and credit cards immediately. If your checking account number and routing number have been compromised, you'll likely have to close the account and open a new one. And don't forget to update any auto-payments tied to those account numbers.

Monitor your credit file. Remember, you get a free credit report, one from each of the three major credit bureaus every year, annualcreditreport.com. This is the only US Federal Trade Commission (FTC) authorized site for obtaining free credit reports. Watch it closely.

Submit a fraud alert with the credit bureaus. With a fraud alert in place, no one can open a line of credit under your name without first verifying your identity. This usually means calling you and asking identifying questions that only you would know. Unlike a credit freeze, you only have to notify one credit bureau and that bureau must notify the other two. Fraud alerts last one year (up from 90 days as of 2018) so you may want to set a calendar alert to remind you to renew the alert in a year's time. As a victim of identity theft, you can request a seven-year fraud alert. A fraud alert also entitles you to a free credit report from each credit bureau, in addition to the three you already get every year.

Submit a credit freeze. Doing so will mostly stop cybercriminals from continuing to open credit accounts under your name. Is a freeze foolproof? Not entirely. In a disturbing report, Brian Krebs found a workaround that could potentially allow criminals to lift a freeze on your credit with only your name, Social Security number and birthday. And in the case of most Americans, all three are readily available for sale on the Dark Web.

Watch your inbox carefully. Opportunistic cybercriminals know that millions of victims of any given data breach are expecting some kind of communication regarding hacked accounts. These scammers will take the opportunity to send out phishing emails spoofed to look like they're coming from those hacked accounts in an attempt to get you to give up personal information.

Consider credit monitoring services. As mentioned previously, if the service is free, go ahead and sign up. Otherwise, consider monitoring your own credit.

Contact the Consumer Financial Protection Bureau (CFPB). You have a legal right under the Fair Credit Reporting Act to dispute any incorrect information on your credit report. The reporting agency has 30 days to investigate your dispute and let you know the results. If the reporting agency doesn't fix or remove the fraudulent activity, you can turn to the CFPB and file a complaint. Hopefully, you won't have to take this step, but it's nice to know there's a government agency looking out for consumers.

Use multi-factor authentication (MFA). Two-factor authentication is the simplest form of MFA, meaning you need your password and one other form of authentication to prove that you are who you say you are and not a cybercriminal attempting to hack your account. For example, a website might ask you to enter your login credentials and enter a separate authentication code sent via text to your phone.

And that's it for this week and hope you all have a great weekend and also wishing my Canadian friends a happy Victoria day long weekend.

Alastair