In this issue:

- **How to avoid identity theft this tax season**
- **Cybersecurity shorts**
- **Software updates**

Dear <first name>,

Welcome to your February Savvy Cybersecurity newsletter. As always, we saw many cybersecurity happenings this month including breaches at Sprint, Google Photos, and more. Read on to learn about those stories as well as:

- An update on the Equifax breach
- What you must do to your Google Nest devices
- A new USPS scam making the rounds
- And more

How to avoid identity theft this tax season

Tax identity theft has been on the decline in recent years due mostly to education and outreach, but many individuals, businesses, and tax preparers still fall victim to tax-related fraud every year. This type of fraud can vary from fraudulent tax returns to phishing messages asking for tax information. Last year, there was a spike in phishing messages sent to tax preparers attempting to get client information.

This year, the Internal Revenue Service (IRS) has created Identity Theft Central, a new webpage to help individuals, businesses, and tax preparers prevent tax identity theft and handle it if one does fall victim. The more knowledge you have on these types of scams and fraud, the less likely the scammer will succeed. As we enter the rush of tax season, be sure you know how to avoid identity theft this year.

1. Be aware of popular scams

Phone scams are one of the most common scams deployed by identity theft fraudsters. You have likely received one of these fake calls over the years appearing to be from the IRS and demanding money for tax debts. The scammers create a sense of urgency and fear that results in many giving over money or personal information. It is important to remember that the IRS will contact you via letter if there is something wrong with your tax information—not over the phone.

Phishing messages are also a widely used method of scamming taxpayers. These messages may appear to come from the IRS or even your bank or tax preparer. For instance, some consumers reported receiving phishing emails from their tax preparer last year that either asked for personal information or requested that they download an attachment. Again, remember that the IRS will not contact you via email. If you receive something from your bank or accountant, be sure to call and confirm that they really sent it.

2. Know the signs of tax identity theft

In many cases, you may not realize that you are a victim of tax identity theft until you go to file your taxes and cannot or you are notified by the IRS. If you file your taxes and are told that you have already filed, you must contact the IRS right away.

You may be able to catch the scammer before they complete the fraud by looking out for some warning signs: for example, if you receive a tax transcript in the mail that you did not request or if you are notified of an online account that you did not set up. If this occurs, again you must contact the IRS immediately.

3. Protect your identity and devices

Certain individuals who have experienced identity theft before or live in a particular state may be eligible for the IP PIN program. This was first introduced a few years ago and acts like two-factor authentication for filing taxes. Once you are assigned a PIN, you (or your tax preparer) will need to enter it before you can file your taxes. Visit this site to see if you are eligible.

Individuals, businesses, and tax preparers all need to protect their devices this tax season—that means mobile phones, computers, and tablets. Individuals should be sure that they are using secure Wi-Fi and devices when filing taxes online or communicating with their tax preparer. Use strong and unique passwords for any sites that contain your personal information and be on the lookout for phishing emails. Tax preparers need to follow the same guidelines and also be sure they are encrypting and protecting client data.

Don't let this tax season be a win for the scammers! Be on the lookout for scams and when possible, file early, as it reduces your chances of fraud.

Cybersecurity shorts

Sprint customers' personal data may have been exposed online. The mobile provider reported that some posts made on a private customer support forum were accidentally made public on the Internet. These posts often include information such as name, device identifiers, and location information. No payment card data is believed to have been exposed.

Your videos may have been sent to strangers if you use Google Photos. Google is alerting some users that a technical issue resulted in private videos being sent to others on the platform over a few days in November. Google has not said how many users were affected or how many videos were exposed. If you were impacted, you likely already would have been notified by Google.

Canadian federal departments and agencies have exposed information on over 140,000 consumers over the past two years. This information was included in a report last month which also found that not all consumers were informed of any breached information. The Canada Revenue Agency had over 3,000 incidents that put consumer information at risk. Health Canada had over 100 breaches affecting 20,000

Canadians. Those who believe their information may have been exposed can file complaints with the commissioner.

Chinese intelligence officers charged by U.S. in record-breaking Equifax hack. The credit bureau was breached in 2017 and exposed information on over 150 million consumers. This month, federal prosecutors announced charges against four Chinese spies. A grand jury indicted the individuals with wire fraud, economic espionage, and conspiracy to commit computer fraud.

Census Bureau experiencing cybersecurity issues in lead-up to census count. For the first time, the majority of census information is poised to be collected online. However, a recent test found that not enough users were able to use the app at the same time. The bureau is now using a backup system that has not been thoroughly tested.

IRS launches "Identity Theft Central" webpage to help combat tax fraud this filing season. This page has resources for consumers, businesses, and tax professionals. For individuals and businesses, you can learn how to protect your information and what to do if you are a victim. Tax professionals can learn what to do if their firm is a victim and how to protect client data.

US Postal Service phishing email makes the rounds. The email appears to come from the Postmaster General and alerts recipients that they have a $100,000 package waiting to be delivered. The email asks for personal information so the package can be delivered. The USPS has said this email is a scam and the agency will never reach out directly to demand money.

Social Security scam is now the most common way to defraud the elderly according to a new Senate report. During this scam, the victim receives a phone call appearing to come from the Social Security Administration alerting them that their Social Security number has been suspended due to suspicious activity. In order to reinstate their Social Security number, they must provide financial information and transfer thousands of dollars. Later, it is discovered the call came from a fraudster. The Social Security Administration has increased public outreach to help combat this scam.

Citrix Systems had its networks compromised for five months between 2018 and 2019 when hackers were able to gain access and steal information and data. The hack was first announced a year ago, but Citrix has just now shared that hackers were able to access financial data on employees, contractors, interns, and job candidates. This information may include Social Security numbers, driver's license numbers, financial account information, health insurance claims, and more. Citrix notified affected individuals on February 10, 2020 via letter.

Iowa Caucus app was vulnerable to hacking say security experts. IowaReporterApp caused issues during this month's caucus after a glitch caused delays in results, but the issues could have been much worse. Veracode, a security firm, reviewed the software and found that hackers could have broken in and intercepted or changed vote totals, passwords, and other information. There is no evidence that the app was hacked, but it is concerning that such a vulnerable software was used in our elections.

Google Nest to require two-factor authentication for users later this year. The company produces smart-home items such as speakers, thermostats, and smoke detectors. Nest always offered two-factor authentication, but it was previously optional. This move comes after Amazon Ring devices were hacked due to poor user security. Both Nest and Ring will soon require two-factor authentication for all devices.

Google begins crackdown on insecure file downloads. Beginning next month, Chrome will begin warning users when they are downloading anything over an HTTP connection. These files can put your security and privacy at risk. It is often difficult to identify these downloads because the website may be secure (HTTPS) while the download itself is not. In October, Google will block all downloads via HTTP.

Software updates

Adobe: Adobe released updates for Flash and Reader this month. The update for Flash is considered critical and should be updated immediately. Flash will be retired later this year so if you no longer need the program, delete it. You can learn more about the update here.

Microsoft: Microsoft released updates this month closing 100 security issues. These flaws affected Windows operating system, Internet Explorer, Microsoft Exchange, and other programs. The Internet Explorer flaw is considered critical and is currently being exploited. You can learn more about the updates here.