Loyola Credit Union
People Helping People

NCUA
Federally Insured by NCUA.

In the Wake of a Major Data Breach

Following the news of the massive data breach, other scammers have come out of the woodwork finding new ways to take advantage of the publicity surrounding the hack.

Below are a few scams to be on the lookout for.

The IRS warns taxpayers about **Tax Refund Fraud**.

These scams involve criminals getting victims' names, addresses and Social Security numbers **to file fraudulent tax refund claims**. Victims don't become aware of a problem until they file their annual tax returns and the IRS notifies them that another return has already been filed and their refund has been claimed.

If your information was compromised in the data breach, ***make a point of filing your annual tax return as early as possible***.

Take immediate action if you are informed that:

- ***More than one return was filed in your name***;
- ***You owe additional tax***; or
- ***IRS records indicate that you earned more than the amount of wage you reported***.

What action should you take? File a police report and a fraud report with the FTC Identity Theft Hotline (877-438-4338). Also complete IRS form 14039, the Identity Theft Affidavit. You may be forced to file your tax returns on paper in the meantime. If you do not get a prompt response from the IRS, call the Identity Protection Specialized Unit at 800-908-4490 for assistance.

The Federal Trade Commission is warning consumers about **Imposter Scams**.

Someone calls you saying, "This is Equifax calling to verify your account information." Stop. Don't tell them anything. They're not from Equifax. It's a scam. Equifax will not call you out of the blue.

That's just one scam you might see after Equifax's recent data breach. Other calls might try to trick you into giving your personal information.

- ***Don't provide any personal or financial information*** unless you've initiated the call.
- ***Don't trust caller ID.*** Scammers spoof their numbers so it looks like they are calling from a particular company.
- ***If you get a robocall, hang up.*** Don't press 1 to speak to a live operator or any other key to take your number off the list. If you respond by pressing any number, it will probably just lead to more robocalls.

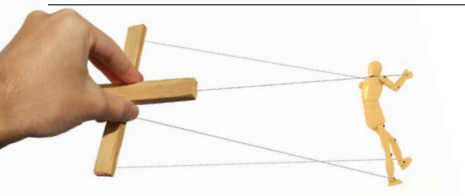
If you've already received a call that you think is fake, report it to the FTC. If you gave your personal information to an imposter, it's time to change any compromised passwords, account numbers or security questions. Visit IdentityTheft.gov to learn how you can protect yourself.

Spear-phishers appear to be someone you know or trust.

The data made available through the Equifax breach is likely to spur a wave of ***"spear-phishing"*** attacks. Unlike regular phishing attacks, these are personalized to their victims. Because of the personal level of these emails, it is more difficult to identify spear-phishing attacks. With all of this information, the attacker would be able to act as a friend or a familiar entity and send a convincing but fraudulent message to increase their chance of fooling recipients into giving up information or clicking on a link.

The best advice after the Equifax breach is to assume any communication is suspect.

- ***Don't post it on social media*** if there is anything that you do not want a potential scammer to see.
- ***Don't click on the links***. If an organization, such as your financial institution, sends you a link, launch your browser and go directly to that site instead of clicking on the link itself. You can also check the destination of a link by hovering your mouse over it. If the URL does not match the link's anchor text or the email's stated destination, there is a good chance that it could be malicious.
- ***Don't use the same password*** for more than one account & change them frequently.
- ***Frequently update your software.*** Enable ***automatic software updates*** when possible.
- ***Use logic.*** If you get an email from a "friend" asking for personal information including your password, carefully check to see if their email address is one that you have seen them use in the past. Real businesses will never send you an email asking for your username or password.



Social Engineering is a Human-On-Human Con

Technology can help protect you from social engineering on the Internet, so pay attention to warnings and alerts from your security software. It is important you recognize that, while most people who call or email you are generally not attempting to swindle you, there is a possibility that they are. This means that you need to understand that not every email is safe; not every caller is who he says he is; not every person knocking on your door is harmless; and not everyone who walks into your place of business has honest intentions.

Make Yourself a Harder Target

The Equifax data breach that was revealed September 7 is more significant than any other major breach because of the nature of the data that was exposed. Equifax has estimated the hack impacts 143 million people, exposing names, Social Security numbers, birth dates and addresses, and many driver's license numbers, credit card information and dispute documents that included more personally identifying information.

All of this information is perpetually valuable to cyber criminals. They could eventually sell your data to other criminals who could then use it to take out loans or credit cards in your name, steal your tax refund, access your medical benefits and countless other crimes for years to come.

Don't get complacent. Stay vigilant. Criminals have extraordinary patience. Thieves may have access to your identity long before they actually commit any fraud.

Here are some do's and don'ts to help reduce your fraud risk.

Do's:

- ***Check your credit report regularly*** for any signs of identity theft.
- ***Place a fraud alert on your credit report*** if your data has been compromised.
- ***Consider placing a security freeze on your credit report.***
- ***Use security software with a firewall and anti-virus.*** Set it to update automatically.
- ***Keep your software up to date*** (browser, applications, operating systems).
- ***Monitor your bank and credit card statements often.*** Sign up for monitoring alerts when possible.
- ***Use strong passwords*** and change them frequently.
- Look for the following in your browser address bar: ***"https", lock icon, green text or shading.***
- When it's tax season, ***file early***. And make sure your tax records are secure.
- For accounts that support it, ***turn on two-factor authentication***.
- ***Keep an eye on your medical insurance benefit statements***.
- ***Beware of breach-related scams***.
- ***Check your security settings on social network sites***.
- ***Beware of disaster-related scams***.
- ***Back up your files*** to an external hard drive or cloud storage.
- ***Assume any offer that seems too good to be true*** is probably a fraud.
- ***Report any suspicious activity immediately*** to the respective institution.
- ***Make a call if you're not sure***. Phishers use pressure tactics and prey on fear.

Don'ts:

- ***Don't use unsecured public Wi-Fi*** to access any accounts or to shop.
- ***Don't use the same password for more than one account***.
- ***Don't click on links or downloads*** until you've confirmed it's legitimacy. A hacker can send you to a spook website hoping to trick you into filling out an online form, or they could install malware, keystroke-logging software and other malicious technology that grabs your attention without ever noticing.
- ***Don't share personal information*** such as travel plans, location check-in or birth city ***on social media sites.***
- ***Don't routinely carry your Social Security card.***

Natural disasters keep scammers busy, don't be a victim. You may want to help families left stranded by the hurricanes. Keep in mind, scammers prey on good natured people. Use caution if you get a call asking to donate. You can verify if it's a legitimate organization by visiting **www.Give.org** and see what charities are listed.

Actions to Take If You Become A Victim of Identity Theft

Place a "FRAUD ALERT" on your credit reports, and view the reports carefully. The alert tells creditors to follow certain procedures before they open a new account in your name or make changes to your existing accounts. The three nationwide consumer reporting companies have toll-free numbers for placing an initial 90-day fraud alert. A call to one company is sufficient:

Equifax: **1-800-525-6285**
Experian: **1-888-EXPERIAN (397-3742)**
TransUnion: **1-800-680-7289**

Placing a fraud alert entitles you to free copies of your credit reports. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain.

Federal law allows you to get a **free** copy of your credit report, at your request, every 12 months from each credit reporting company.

www.AnnualCreditReport.com
877.322.8228

CLOSE ACCOUNTS. Close any accounts that have been tampered with or established fraudulently.

- Call the security or fraud departments of each company where an account was opened or changes were made without your okay. Follow up in writing with copies of supporting documents.
- Use the ID Theft Affidavit at **ftc.gov/idtheft** to support your written statement.
- Ask for verification that the disputed account has been closed and the fraudulent debts discharged.
- Keep copies of documents and records of your conversations about the theft.

FILE A POLICE REPORT. File a report with law enforcement officials to help you with creditors who may want proof of the crime.

REPORT THE THEFT TO THE FEDERAL TRADE COMMISSION. Your report helps law enforcement officials across the country in their investigations.

- Online: **ftc.gov/idtheft**
- By phone: **1-877-ID-THEFT (438-4338)** or TTY, **1-866-653-4261**
- By mail: Identity Theft Clearinghouse, Federal Trade Commission, Washington, DC 20589

Hackers use social media sites such as Facebook, Instagram and Twitter to find dates of birth, personal anecdotes or other information that can be used in security questions. This information, along with any personal information that gets exposed through a major data breach, gets a cyber criminal closer to having a person's full financial and medical profile, a hacker's Holy Grail.