COLORADO FINANCIAL MANAGEMENT®

# All Things Financial Planning

*Jason Foster, Director of Financial Planning, JD*

March 2021

**SUMMARY:**

- Introduction: Secure Act 2.0 and Common Tax Deductions and Credits
- Defending Against Cybersecurity Threats

Dear Clients,

With spring on the way and vaccines being rolled out in a meaningful way, we are grateful 2020 is behind us and are optimistic for 2021 and beyond. After a discussion on potential retirement legislation and common tax deductions and credits to consider when filing your tax return, we have dedicated this newsletter to providing information and considerations on cybersecurity and the protection of your money, information, and identity. We have focused on the most common types of cyberattacks and useful defenses to employ to avoid becoming a victim. We finish by discussing what we do at CFM to safeguard your accounts and information, because as you do business with us, we want you to feel secure and be confident that your safety and security is a priority for us.

In late February, a $1.9 trillion economic aid package passed through the House and is now being hotly debated in the Senate. When the final version of the stimulus is passed, there will most certainly be another round of direct payments, as well as additional assistance for the unemployed, tax credits for families, funding for state and local governments, and assistance for people on the verge of losing their homes. Expect monetary provisions assisting small businesses as well, which may be more targeted than the first round of stimulus capital released last year.

**SECURE ACT 2.0.** With Covid-19 relief a priority and the economy still fragile, I believe tax policy changes are unlikely for 2021 (but a real possibility for 2022). Another version of the SECURE ACT, however, could be in the works this year due to significant bipartisan support. **Potential key changes** effecting retirement plans already gaining momentum are as follows:

- An increase in the "catch-up" IRA contribution amount for individuals age 60 or over to $10K
- An increase in the starting age for RMDs to 75
- Individuals with an aggregate balance of under $100K in their retirement accounts would be exempt from the RMD rules
- Qualified Charitable Deductions from retirement accounts would be expanded to include distributions from employer plans and increased to $130K
- There would be a reduction in the penalty for failing to take RMDs to 25% (versus 50% currently)

While other provisions such as auto enrolling new employees into retirement plans at 3% and providing matching contributions to 401ks, 403bs, 457bs, and

Simple IRA plans on behalf of employees who are electing to repay student loans instead are possible, the above listed provisions are gaining the most support and will likely pass as new legislation.


The **tax filing season** is upon us and there are still tax savings options to consider before the April 15th deadline. For IRAs, up to $6000 can be contributed if you are under 50. For those of you 50 and over, you can add $7000 to your IRAs. If you have a high-deductible health insurance plan that makes you eligible for a health savings account, you can make tax-deductible contributions for 2020 until April 15th. The max contribution to a health savings account for 2020 is $3550 for self-only coverage and up to $7100 for family coverage, although those over age 55 can contribute an additional $1000 as a "catch up" amount.

For self-employed individuals, if you have opened an account prior to December 31, you can still contribute to your solo 401k or SEP IRA up to $57,000 (plus a $6000 catch-up contribution for those 50 or older) up to tax filing deadline.

**Other Tax Deductions and Tax Credits.**
Although most taxpayers now take the standard deduction of $12,400 for single filers, $24,800 for married taxpayers, and $18,650 for heads of household, it is worth reviewing your total deductions to see if it is still beneficial to itemize. Here are some of the largest and most common itemized deductions to consider:

- **Student loan interest deduction** – up to $2500 from your taxable income if you paid interest on your student loans
- **Mortgage interest deduction** – the mortgage interest paid on the first $1 million of mortgage debt (if purchased prior to 12/15/2017; otherwise $750K is the limit)
- **State and local tax deduction** – up to $10,000 for a combination of property taxes and state and local income taxes or sales tax
- **Charitable donations deduction** – a dollar for dollar deduction for gifts made to charity (you also can deduct $300 on your tax return for gifts to charity, if you are utilizing the standard deduction)
- **Medical expense deduction** – for qualified, unreimbursed medical expenses of more than 7.5% of your adjusted gross income for the tax year
- **Home office deduction** – with Covid-19 forcing more people to work from home, if you utilized your home regularly and exclusively for business-related activity, it is possible the IRS will let you deduct associated rent, utilities, real estate taxes, repairs, maintenance and other related expenses. Although this possible deduction is gaining greater popularity, you will want to consult your CPA about it's applicability in your situation.

You can apply **tax credits** regardless of whether you itemize or take the standard deduction. Popular tax credits include:

- **Child tax credit** – receive up to $2000 per child as a credit on your return
- **Child and dependent care tax credit** – up to $6000 of expenses for 2 or more dependents
- **Earned Income Tax Credit** – worth between $538 and $6660 depending on many children you have, your marital status and your income level
- **American Opportunity Credit** – covering each of the first 4 years of college, a credit of $2500 per qualifying student is available for tuition and fees (qualification based on income level)
- **Lifetime Learning Credit** – covering any years of post-secondary education (not just the first 4 years), a credit of $2000 is available per return (qualification based on income level)

Although we are not CPAs, we are happy to have a conversation with you about whether a specific deduction or tax credit may apply. We can also connect you with local accountants who can provide advice and assist you with the filing of your return.


**"I reviewed your investments and set you up for early retirement. On your last day of work, you can afford to leave at 4:30 instead of 5:00."**

---

**Defending Against Cybersecurity Threats**
By Shannon Knight Howell, Associate Financial Planner

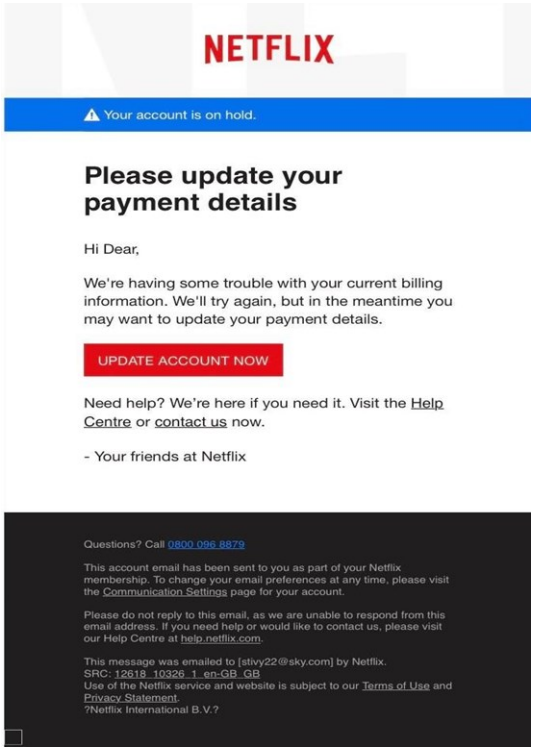
From banking to social media accounts, more and more of our information is online and at risk. With online crime increasing and tactics evolving, vigilant cybersecurity countermeasures are the best way to protect yourself from an unprecedented attempt at stealing your information, identity, and money.

And it's not getting any easier. According to the cybersecurity firm McAfee, losses from cybercrime hit a record high of $945 billion in 2020, just over 1% of global gross domestic product. This statistic is a sobering reminder that we all must continue to remain on the defensive as we face increasing attacks.

COVID-19 has only exasperated the issue, moving classrooms, jobs, and roles remotely and online, creating more opportunities for cyberhackers to try and gain access to online accounts. Since the pandemic began, the FBI has reported a 300% increase in reported cybercrimes according to a recent Cybint Solutions article. And, of course, Cybercrime goes beyond a dollar amount lost. Opportunity costs and time and money spent to defend against and fix any potential hacks or blind spots are some of the casualties that are not associated with actual dollars lost, but nonetheless an important consideration in cybercrime.

Cyber threats can come in various forms, but all efforts are utilized to steal valuable information that can be used in various identity theft schemes. Here are a few of the most common methods that can be utilized against you:
- Phishing
- Credential Replay
- Social Engineering
- Email Account Takeover
- Malware

**Phishing** is one of the most common practices amongst cybercriminals, as 79% of cyberattacks combine some type of phishing and hacking. Through a "phishing" scheme, fraudsters pretend to be a trustworthy source in order to acquire sensitive personal information such as usernames, passwords, social security numbers, and credit card details. A form of social engineering, phishers target individuals via text message, phone, or email, posing as a legitimate source or known sender asking or luring individuals to provide your personal information in order to access your accounts. The phishing scam can often appear as a hyperlink embedded in an email that an individual clicks on and directs them to a legitimate looking website to enter in their credentials. You may get what appears to be a legitimate email from your bank or your favorite retailer, notifying you of suspicious activity or login attempts on your account, or telling you there is a problem with your recent payment. Here is a real-world example from the federal trade commission's website:


NETFLIX

Your account is on hold.

**Please update your payment details**

Hi Dear,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

UPDATE ACCOUNT NOW

Need help? We're here if you need it. Visit the Help Centre or contact us now.

- Your friends at Netflix

Questions? Call 0800 096 8879

This account email has been sent to you as part of your Netflix membership. To change your email preferences at any time, please visit the Communication Settings page for your account.

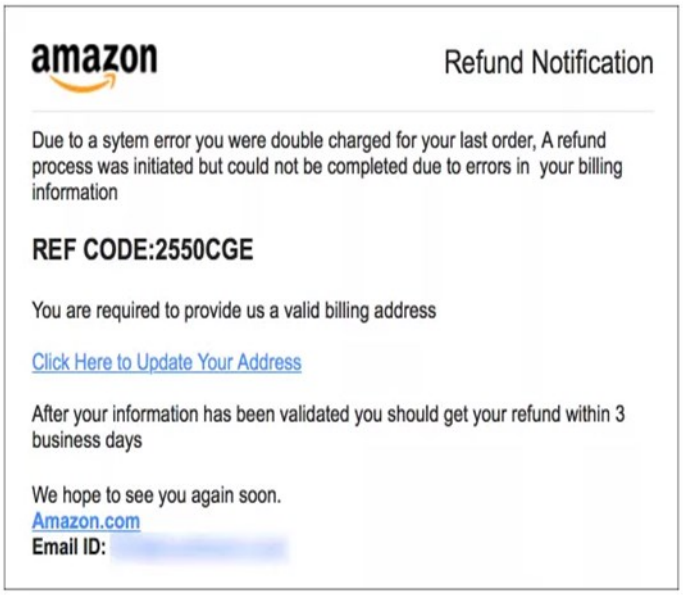
Please do not reply to this email, as we are unable to respond from this email address. If you need help or would like to contact us, please visit our Help Centre at help.netflix.com.

This message was emailed to [stivy22@sky.com] by Netflix.
SRC: 12618_10326_1_en-GB_GB
Use of the Netflix service and website is subject to our Terms of Use and Privacy Statement.
?Netflix International B.V.?

This email looks like it is from a company we all know and trust. It even uses a Netflix logo and header. But the "Hi Dear" generic intro is a sign that you should be careful. Reading further, the "Help Centre" link should cause you even more concern. Should you click on the red button? No. Instead, go directly to Netflix's website with this information and login to discover if there is any legitimacy to the claim. Or call them.

According to Norton, a company that specializes in combating cybercriminal tactics, a bank or credit card provider will never ask you to provide account information online. When emails ask for this information, it's the first sign the email is a phishing scam. You can check the links that these emails ask you to click, too. If you hold your cursor over them, you'll see their true addresses, and if they are a fake, they likely will not be affiliated with the bank or credit card provider they are attempting to emulate. Other tell-tale signs? Look for grammatical errors or odd sounding phrases or sentences in the text and a low-resolution logo. Here is another example:


Just like a bank or credit card company, the IRS will never email you to ask for your personal information. The IRS only communicates about taxes owed or a refund coming your way via mail. If you get a message saying that the IRS owes you money, call them. Odds are high that the IRS doesn't owe you anything (because you didn't receive that aforementioned letter) and that this was a phishing attempt to scam you. Avoid clicking on the link at all costs.
Check out this last example:




I doubt Amazon, one of the largest and most sophisticated companies on earth, would have a problem spelling "system" in the first line of a message to you. If you have your doubts – call them or log into your account directly through their website. If you were double charged on your last order, they will have a notice within your account.

**Credential Replay.** When cybercriminals obtain login credentials, they can test them in large numbers against financial institutions' websites to find matches, and then request fraudulent fund transfers. They also resell this information for a profit to other cybercriminals, who wish to use this information to commit fraud. This is called credential replay. If the cybercriminal is not stealing these credentials themselves, they can easily purchase large numbers of stolen login credentials from the dark web. These large volumes of credentials typically come from large data breaches you have read about (or have become a victim of) in the news – think Equifax, Yahoo, LinkedIn, Home Depot, etc.

One of the best, most effective ways to avoid being the victim of a cybercrime is to **use a**

**variety of complex passwords and change them frequently.** Use at least 8-12 characters, upper and lowercase letters, and symbols. Change your password every 90 days. Do not use your social security number, birth date, other personal data when creating passwords, or other information that can be easily found online about you. Below is an exercise designed to make you consider twice before using easily obtained information online (even your pet's name!).


**Social Engineering** involves the psychological manipulation of people in order to establish a level of trust that leads to the victim taking action. Cybercriminals attempt to befriend you over time until they are able to solicit sensitive information from you to commit the fraud…and then they disappear. They can utilize phone, email or even social media to defraud you.

The best way to avoid being a victim of social engineering is to be cautious and protective about the information you choose to share on social media. Keep your personal information private (do not share your home address, phone number, employer, vacation dates, and birthdate).

**Email Account Takeover.** This occurs when a cybercriminal hacks an email account and searches for emails involving correspondence between the client and their financial institutions (like us). The goal is to learn about the victim and their habits so they can pose as the victim to steal money – by impersonating the client and providing instructions within the email to transfer funds to a fraudulent account. To defend against this tactic, CFM directly verifies the identity and all such requests from the client.

**Malware software** is created to damage and disable computers and computer systems, steal data or gain unauthorized access to networks. Examples of this include viruses, worms, Trojan horses, ransomware, and spyware. They are most commonly installed on a computer when a user clicks an unsafe link, opens an infected file, or visits a legitimate website that could contain these types of software. Malware can delete files or directory information, or it may allow attackers to covertly gather personal data, including financial information, usernames and passwords.

To shield against unwanted Malware on your computer:

- Do not click on suspicious links
- Do not open attachments or click on URLs in unsolicited emails, even from those you know
- Do not insert any USB device that you have received from an unknown/unreliable source.

**Protecting your Schwab and Fidelity Accounts from Cyberhackers**

With the cybersecurity road a treacherous one to navigate on your own, thankfully many large financial institutions, such as our custodians Schwab and Fidelity, have taken steps to help clients safeguard account information, and have encouraged clients to sign up for measures that can help thwart hacking attempts. You can **set up security and activity alerts with these institutions**, where they can notify you by text or email of any money movement, password changes or other updates to your personal information or accounts. Thus, if you received a notice that money is being transferred or that your password has been changed, and you didn't initiate this action, you'll need to contact your financial institution immediately.

Both Schwab and Fidelity also now encourage the use of **Two-Factor Authentication (2FA)**. 2FA is an extra layer of security that is added to your account to prevent someone from logging in, even if they have obtained your username and password. First, an account holder would enter in their username and password. Then instead of immediately gaining access, another step would be required to access the account. Once this secondary information is obtained, the second factor of authentication would be provided, and the account holder can then access the account. 2FA can come in several forms:

- **Token number:** A token will generate a numerical code to enter before you are able to access your accounts. This most commonly is utilized through a security app on your phone, generating a new code every 30 seconds or so.
- **Other personal information:** This can come in the form of a personal identification number (PIN), an additional password, an answer to a "secret question", or a series of keystroke patterns.
- **Proprietary:** This type of identifying personal property is more advanced, involving a fingerprint, an iris scan, or voice recognition.

The use of 2FA makes hacking your accounts much more difficult because another piece of information is required. Charles Schwab and Fidelity both offer 2FA in the form of a token, and will gladly take you through the steps of setting it up. Charles Schwab also offers a verbal password to access accounts when you are calling in to the Schwab Alliance Line. You can contact Schwab Alliance directly at 800-515-2157 to establish this layer of protection.

* * *

Here at CFM we work incredibly hard at providing a safe and secure business platform by developing sound, protective business practices safeguarding your money and information. We review these policies and procedures frequently to guarantee consistent implementation by our staff, and to make sure we are adopting the latest and most effective tactics to combat these evolving outside cyber threats. We have adopted our own version of two factor authentication when accessing your accounts to trade, or accessing your files to work on a financial plan. When sending and receiving emails that contain documents with confidential information, we utilize a secure email format called Citrix to protect against this information being exposed. Client meetings via Zoom require either a passcode or have waiting rooms enabled for meeting hosts to admit the proper parties to the meeting. Quarterly Statements are sent PDF password protected and secured. For those that utilize our financial planning software, eMoney, we encourage the use of a secure "Dropbox" called the "Vault," which acts as a secure place to share documents with our financial planning team online.

If you have further questions about the safeguards we employ, let us know – we are happy to have this conversation. As always, your confidence and trust are of the highest importance to us. Stay safe and be vigilant.

---

The Financial Planning Department
***And Your Entire Colorado Financial Mgmt. Team***


COLORADO FINANCIAL MANAGEMENT®

303-443-2433 ww.colofinancial.com

Boulder
4840 Pearl East Circle, Suite 300E
Boulder, CO 80301

Denver
3033 E First Ave, Suite 408
Denver, CO 80206

Loveland
4848 Thompson Pkwy, Suite 320
Johnstown, CO 80534