Winter 2022

Financial planner

PARK PLACE WEALTH ADVISORS, INC.

DANIEL J GANNETT & JEAN C. GANNETT, CFP®

· 18 ORINDA WAY ORINDA, CA 94563 ·

· 505 W OLIVE AVE, SUITE 305 SUNNYVALE, CA 94086 ·

DAN@PARKPLACEWEALTH.COM

JEAN@PARKPLACEWEALTH.COM

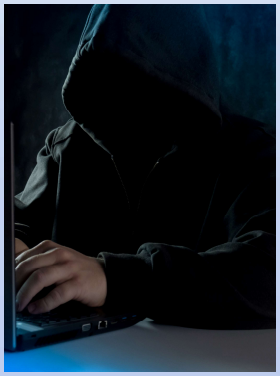
· ORINDA – (925) 254-7766 ·

· SUNNYVALE – (408) 733-0245 ·

· FAX: (925) 258-0591 ·

Winter 2022 Newsletter Topics

- *Being Safe Online*
- *How to Withdraw Money from your 529*



Being Safe Online

Unfortunately, Cyber fraud is on the rise: we all see reports reularly about data breaches and cyber frauds. To protect you, we are commited to keeping your accounts safe and verifying all requested transactions with a phone call. Please use these pratical tips to stay safe online.

Common tactics used to steal login credentials

Some of the most common tactics criminals use to compromise a victim's identity or login credentials are described below. After gaining access to an investor's personal information, criminals can use it to commit various types of fraudulent activity. The action items presented in the investor protection checklist are intended to help you and your family better protect yourselves against such activity.

Malware Using malicious software (hence, the prefix "mal" in malware), criminals gain access to corporate and private computer systems and gather sensitive personal information such as Social Security numbers, account numbers, passwords, and more.

How it works: While malware can be inserted into a victim's computer by various means, it often slips in when an unwary user clicks an unfamiliar link or opens an infected email attachment. **Tip:** If you don't recognize the sender, don't click on it!

Phishing Phishing is a popular tactic used by cyber criminals to steal account information or login credentials. It is essentially a fake electronic message designed to trick you into divulging information and/or granting access that you shouldn't. This is often accomplished with the help of a fake website that strongly resembles a real site. Social Network surveys are a type of phishing where a hacker may be trying to gain personal information.

How it works: Masquerading as a known entity, or one with which the victim may have a financial relationship (e.g., a bank, credit card company, brokerage company), criminals lure victims into opening email links or attachments. Doing so may direct victims to provide sensitive information on a fake website, or it may install malware to capture login and account information. TIP: Don't click links in emails to connect to banks or other financial institutions. Only go directly to their known login sites.

Credential Replay It's common practice for people to use one password on many sites. However, doing so leaves people vulnerable to credential replay attacks.

How it works: Attacks occur when a criminal obtains the password for one compromised account and then tries to use it to log in to other accounts. The more a password is reused, the more chances there are for that password to be compromised or stolen. Tip: Change Passwords often!

Park Place WEALTH ADVISORS, INC.

INSIGHT:

Since 1946, there have been 84 declines of 5% to 10% in the S&P 500, which works out to more than one a year. The average time it takes to recover from those losses is one month. *CNBC, January 25, 2022*

As always, we encourage investing with your goals in mind, keeping a reserve for emergency needs.

We are available for in person, phone or zoom reviews. Give the office a ring and we can discuss your investing goals and needs.

Investor protection checklist

The educational checklist presented below is designed to help you take appropriate action to better protect you and your family and mitigate risk of cyber fraud. Carefully review the items in each of the categories below to determine which apply to your unique situation.

Manage your devices.

- Install the most up-to-date antivirus and antispyware programs on all devices and update these software programs as they become available. These programs are most effective when users set them to run regularly rather than just running periodic scans, which may not provide maximum protection to your device.
- Access sensitive data only through a trusted device and secure Internet connection; avoid use of public Internet connections other than through a Virtual Private Network (VPN).
- If you have children, set up a separate computer they can use for games and other online activities.
- Keep operating systems and software up to date (PCs, laptops, tablets, smartphones). Many updates are made to resolve recently identified security risks.
- Do not install pirated software. It often contains security exploits.
- Frequently back up your data in case of ransomware attacks.

Six Ways to Protect Against Cyber Fraud

Protect all passwords.

- Avoid storing passwords in email folders or un-encrypted files on your computer. Consider using a password manager program instead. These programs help generate and manage complicated passwords.
- Use a personalized custom identifier for financial accounts you access online. Never use your Social Security number in any part of your login activity.
- Regularly reset your passwords, including those for your email accounts. Avoid using common passwords across a range of financial relationships and avoid using a single password across multiple sites.
- Utilize multi-factor authentication, especially for financial and email accounts.

Surf the web safely.

- Exercise caution when connecting to the internet via unsecured or unknown wireless networks, such as those in public locations like hotels or coffee shops. These networks may lack virus protection, are highly susceptible to attacks, and should never be used to access confidential personal data directly, without the proper protection of a secure VPN connection.

Protect information on social media.

- Limit the amount of personal information you post on social networking sites. Never post your Social Security number (even the last four digits). Consider keeping your birthdate, home address, and home phone number confidential. We also discourage clients from posting announcements about births, children's birthdays, or the loss of loved ones. Sharing too much information can make you susceptible to fraudsters and allow them to quickly pass a variety of tests related to the authentication of your personal information. Never underestimate the public sources that criminals will use to learn critical facts about people.

Park Place WEALTH ADVISORS, INC.

Park Place Wealth Advisors, Inc.

Daniel J Gannett
Jean C Gannett, CFP®

Orinda Location:
18 Orinda Way
Orinda, CA 94563
(925) 254-7766
Fax (925) 258-0591

Sunnyvale Location:
505 W. Olive Avenue
Suite 305
Sunnyvale, CA 94086
(408) 733-0245

Protect your email accounts.

- Delete any emails that include detailed financial information beyond the time it's needed. In addition, continuously assess whether you even need to store any personal and financial information in an email account.
- Use secure data storage programs to archive critical data and documents.
- Review unsolicited emails carefully. Never click links in unsolicited emails or in pop-up ads, especially those warning that your computer is infected with a virus requesting that you take immediate action.
- Establish separate email accounts for personal correspondence and financial transactions.
- Choose a unique password and utilize multi-factor authentication.
- Review all emails carefully before clicking on links or attachments.

Safeguard your financial accounts.

- Consider contacting the three major credit bureaus to add a "security freeze" and prevent new accounts being opened in your name:
  Equifax: 800-685-1111
  Experian: 888-397-3742
  Transunion: 888-909-8872
- Lock down personal credit reports with Experian®, TransUnion®, and Equifax®. Proactively enroll in an identity theft protection service to protect personal data.
- Review all your credit card and financial statements as soon as they arrive or become available online. If any transaction looks suspicious, immediately contact the financial institution where the account is held.
- Never send account information or personally identifiable information over email, chat, or any other unsecured channel.
- Suspiciously review any unsolicited email requesting personal information. Further, never respond to an information request by clicking a link in an email. Instead, type the website's URL into the browser yourself.
- Avoid developing any online patterns of money movement, such as wires, that cyber criminals could replicate to make money movement patterns appear more legitimate.

How to Withdraw Money from your 529

What can I pay for with my 529 savings plan?

One of the best things about your 529 savings plan is that you can use it to cover a variety of education expenses. In addition to tuition and mandatory fees, the following expenses are generally considered qualified if used while the beneficiary is enrolled at an eligible educational institution:

- Required books, supplies and equipment
- Computers and peripheral equipment (such as printers)
- Computer software, internet access and related services

How to avoid tax penalties

Avoid tax penalties by only using the money for qualified expenses. Money used for anything else will be subject to a 10% federal tax penalty on the earnings and in addition, federal and, if applicable, state income tax. Also make sure your withdrawal matches the payment year of the qualified education expense. Discuss any potential exclusions with a tax advisor.

Be aware that states take different approaches to the income tax treatment of withdrawals. For example, withdrawals for K–12 expenses may not be exempt from state tax in certain states.

Be sure to save your receipts and documentation for tax time!

The account owner or beneficiary is responsible for confirming an expense is qualified. Consult a tax advisor with any questions.

Park Place WEALTH ADVISORS, INC.

A MILLION LESS

In the fall of 2019 (pre-pandemic), 15.47 million undergraduates were enrolled in college.

In the fall of 2021, 14.44 million undergraduates were enrolled (Source: National Student Clearinghouse Research Center)

How can I withdraw funds from my 529 account?

Contact your financial professional to send the money directly to:

- College or university by check
- Bank account on file
- Yourself by check
- Beneficiary (student)

If you need to link a new bank account, there is a 10-day wait before you can send money to the new bank.

To prevent processing delays, verify the:

- School's billing address and student ID number
- Bank account has been on file for at least 10 days
- Requirements to transfer funds if the money is needed for another student's expenses

What to expect at tax time?

Tax reporting depends on who receives the money from the 529 withdrawal. If the money is sent to:

- You (the account owner), then the tax reporting will be under your Social Security number.
- The beneficiary (student) or directly to a school, then the tax reporting will be under the beneficiary's Social Security number.

Form 1099-Q will be issued in January of the year following the withdrawal. Any earnings on withdrawals are exempt from federal taxes as long as you use the money for qualified education expenses.

- Consult a tax advisor to determine who should be the recipient of the money — you, the beneficiary, or the school.

Park Place WEALTH ADVISORS, INC.