NAVALIGN
WEALTH PARTNERS

Financial Cybersecurity
GUIDE

In the digital era, the importance of securing online financial transactions and information cannot be overstated. At Navalign Wealth Partners, we prioritize the safety of your financial assets and personal details, understanding that our mutual trust hinges on robust cybersecurity measures. We are committed to protecting your interests against the constantly changing threats in the cyber landscape, recognizing that our collective vigilance is key.

This guide is designed to simplify complex cybersecurity concepts into practical steps you can take to enhance your digital safety. Covering everything from identifying secure websites to effective password management and spotting phishing attempts, we aim to empower you with the knowledge needed to navigate the online financial world securely. Together, we can ensure a safer financial journey for all Navalign clients.

THE FOUNDATION OF SECURE ONLINE ENGAGEMENT

At Navalign, we view the security of your online accounts as a collaborative effort. It's a dynamic partnership that combines our advanced security measures with your informed participation. Our shared goal is to protect your personal and financial information from unauthorized access, ensuring your peace of mind.

ENHANCED SECURITY WITH TWO-STEP VERIFICATION

An Extra Layer of Protection: Two-step verification adds a significant layer of security to your account access. By requiring not only your password but also a unique security code sent to your mobile device or email. This helps to ensure that only you can access your accounts. This process is straightforward to set up and provides substantial protection against unauthorized access.

SET UP A VERBAL PASSCODE FOR ENHANCED SECURITY

Personalized Access: Enhance your security by setting up a verbal passcode with Navalign. Our team will request this passcode before discussing your accounts or accepting any instructions, ensuring that sensitive information is only shared with authorized individuals. This additional measure fortifies your account's security, providing peace of mind in every interaction.

818.728.4500 navalign.com 15910 Ventura Blvd. Suite 1605, Encino, CA 91436

STAY INFORMED WITH SECURITY ALERTS

Proactive Notifications: By signing up for alerts through the Navalign eMoney client website and Schwab website, you can receive immediate notifications about significant account activities. These alerts are designed to inform you of any unusual actions promptly, enabling you to act swiftly and secure your account if necessary.

By understanding and utilizing these foundational security features, you're taking crucial steps toward securing your online financial presence. It's more than just adding layers of protection; it's about fostering a relationship where we navigate the digital financial landscape together. We can equip you with the tools and knowledge, but your active engagement and vigilance amplify these efforts, creating a secure and trustworthy online financial environment.

BEST PRACTICES FOR ONLINE SECURITY

In our journey toward secure online financial management, knowing how to shield ourselves from potential threats is paramount. Here are some everyday habits and practices we encourage you to adopt, making security a natural part of your digital life.

GENERAL VIGILANCE

Be Wary of the Unexpected: Trust your instincts. Unsolicited phone calls, emails, or texts asking for money or personal details often signal a scam. If something feels off, it probably is. Hang up or delete the message and reach out directly to the source using a contact method you trust.

Share With Care: Think twice before sharing sensitive information online, especially in emails. The digital realm is vast, and not everyone in it has good intentions.

Social Media Savvy: Your personal details are like digital gold. Protect them as such on social media platforms by limiting what you share publicly.

Verify Financial Instructions: If you receive instructions for money movements via email, pause. Call the person or organization directly using a contact number you know is genuine to confirm the instructions before acting.

PHISHING AND MALICIOUS LINKS

Spot the Hooks: Phishing attempts often disguise themselves as urgent messages from trusted people and entities. Always verify the source before clicking on any links or downloading attachments.

Regular Checks: Make it a habit to review your email and account statements for any signs of unauthorized activity. Early detection is key to preventing further damage.

Public Spaces, Private Matters: Be mindful of your surroundings when accessing financial information in public. Over-the-shoulder snoops can be just as dangerous as online hackers.

SECURE WEBSITE NAVIGATION

HTTPS is a Must: Always check for "https://" at the beginning of the website address in your browser's address bar. This 'S' stands for secure, indicating that the site you're visiting encrypts data between your browser and the site's server.

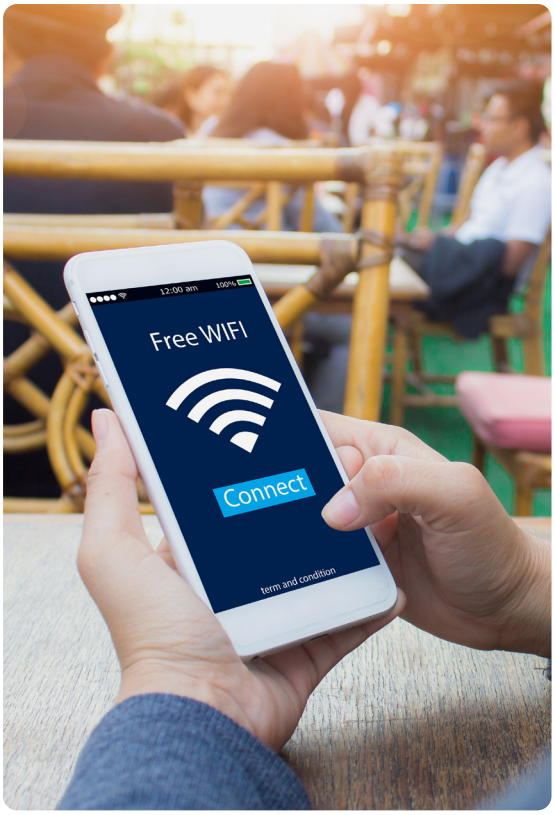
Trust, But Verify: Even on secure sites, stay alert. Look for the padlock icon in your browser's address bar, signaling an encrypted connection.

Log Out, Lock Down: Always log out of websites once you're done, especially on shared or public devices. This simple step can prevent unauthorized access to your accounts.

By weaving these practices into your daily online routines, you're not just protecting your financial assets; you're securing your peace of mind. Remember, in the digital age, a little caution goes a long way.

KEEPING YOUR TECHNOLOGY SAFE

The devices we use daily - computers, smartphones, tablets - are gateways to our financial lives. Ensuring these gateways are fortified can significantly reduce our vulnerability to cyber threats. Here's some tips on how you can keep your technology secure.



UPDATE AND UPGRADE

- **Stay Current:** Regularly update your operating system and applications. These updates often include critical security patches that protect against new vulnerabilities.
- **Antivirus is Essential:** Install reputable antivirus and anti-spyware software on all your devices. Set them to update automatically to combat the latest threats.
- **Secure Settings:** Activate security settings on your web browsers and mobile apps. These settings can help block malicious websites, ads, and protect your data from being easily accessed.

WI-FI WISDOM

- **Public Wi-Fi Caution:** Public networks are convenient but often not secure. Avoid performing financial transactions or accessing sensitive accounts over public Wi-Fi.
- **Personal Hotspots:** Use a personal Wi-Fi hotspot if you need a secure connection on the go. It's safer than an unsecured public Wi-Fi network.
- **Network Security:** At home, ensure your Wi-Fi network is secured with a strong password. Consider also using a network firewall for an added layer of defense.

HARDWARE HYGIENE

- **Device Disposal:** Before disposing of or selling any device, securely erase all data. Consider using professional services that guarantee data deletion.
- **USB Caution:** Avoid using unknown USB drives. They can be infected with malware designed to unlock access to your computer or steal information.
- **Bluetooth Awareness:** Disable Bluetooth when not in use to prevent unauthorized access to your devices.

Taking these steps to secure your technology not only protects your financial assets but also shields your personal information from potential cyber threats. It's about creating a comprehensive defense strategy that encompasses both your physical devices and your online behaviors.

LOGIN CREDENTIALS AND PASSWORD MANAGEMENT

Your first line of defense in the digital world is often your login credentials. How you manage these can significantly impact your online security. Here are some strategies to enhance the safety of your accounts:

UNIQUE AND COMPLEX PASSWORDS

Avoid the Obvious: Never use easily guessable information, like your birthdate or "password," as your password. Attackers often start with the obvious.

Complexity is Key: Create passwords that are a complex mix of letters, numbers, and symbols. The more complex, the harder it is for cybercriminals to crack. This is crucial for accessing financial websites.

A Different Password for Each Account: Using the same password across multiple accounts is like having one key for everything you own. If one account is breached, others could follow. Keep them unique.

PASSWORD MANAGEMENT

Regular Changes: Changing your passwords regularly can help keep your accounts secure. If remembering multiple complex passwords is challenging, consider using a password manager.

Password Managers: These tools can generate, retrieve, and store complex passwords for you. They encrypt your password database with a master password – the master password is the only one you need to remember, as such it should be unique and complex.

TWO-STEP VERIFICATION

An Extra Security Layer: Enable two-step verification, also known as multi factor authentication, wherever possible. This requires not only your password but also a second factor, like a code sent to your phone or email, to access your account.

Use Authenticator Apps: For an even higher security level, use an authenticator app to generate the two-step verification codes. These apps don't rely on SMS or email, and they work even if your phone is offline.

By adopting these practices, you not only protect your accounts but also develop a culture of cybersecurity awareness. It's about making security a routine part of your digital life, ensuring that your financial and personal information remains out of reach from unauthorized access.

SPECIAL FOCUS: Beware of Phishing

Phishing is a prevalent method cybercriminals use to trick individuals into revealing personal information or installing malicious software. By impersonating trusted entities through emails, texts, or phone calls, they aim to steal sensitive data like login credentials, financial information, and more. Here's how to stay one step ahead:

IDENTIFYING PHISHING ATTEMPTS

- **Urgency and Fear:** Phishing messages often create a sense of urgency or fear, prompting quick action. Be skeptical of emails or messages that pressure you to act immediately, especially those requesting personal or financial information.
- **Suspicious Links and Attachments:** Before clicking on any links or downloading attachments, verify the sender's authenticity. Hover over links to preview the URL, and be cautious of those that lead to unfamiliar sites.
- **Look for Red Flags:** Misspellings, grammar mistakes, and email addresses that closely resemble legitimate ones but are slightly altered are common indicators of phishing attempts.

PREVENT PHISHING SCAMS

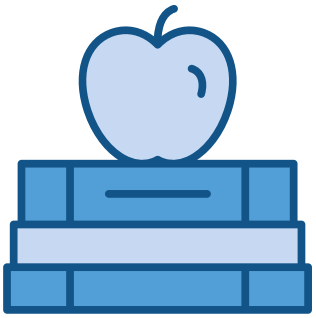
- **Verify Contact:** If an email or message requests sensitive information, validate the request by contacting the company directly through official channels, not by replying to the email or message.
- **Use Spam Filters:** Activate your email's spam filters to help catch phishing attempts before they reach your inbox.
- **Educate Yourself:** Stay informed about the latest phishing tactics. Cybercriminals constantly evolve their strategies, so keeping up-to-date can help you remain vigilant.

WHAT TO DO IF YOU SUSPECT PHISHING

- **Do Not Respond or Click:** If you receive a suspicious email or message, do not interact with it. Do not click on any links or download any attachments.
- **Report It:** Forward suspicious emails to the official email address for reporting phishing in your organization or to the impersonated company. This can help prevent further attempts.
- **Change Your Passwords:** If you suspect you've clicked on a phishing link or provided information to a scammer, change your passwords immediately, especially for any accounts that may have been compromised.

Phishing is a significant threat, but by staying informed and cautious, you can protect yourself from most attempts. Remember, legitimate organizations will never ask for sensitive information via email or text. Always verify requests and stay secure online.

EDUCATIONAL RESOURCES AND ADDITIONAL READING



To further empower you in your journey towards robust online financial security, we've curated a selection of resources that offer deep dives into various aspects of cybersecurity. Engaging with these materials can enhance your understanding and preparedness against the digital threats of today and tomorrow.

STAY SAFE ONLINE

- **What It Offers:** Managed by the National Cyber Security Alliance, this website provides comprehensive resources on protecting yourself, your family, and your devices. Their guidance ranges from securing your home network to safe online shopping practices. (https://staysafeonline.org/)

STOP THINK CONNECT CAMPAIGN

- **Why It's Important:** This global online safety awareness campaign is designed to help all digital citizens stay safer and more secure online. The initiative encourages everyone to understand the risks and offers simple steps to take control of your digital security. (https://www.stopthinkconnect.org/)

ON GUARD ONLINE

- **Focus Area:** Particularly focused on helping parents, teachers, and caregivers navigate the complexities of keeping children safe online. It includes a blog that discusses current cyber trends and offers actionable advice. (https://www.onguardonline.gov)

FDIC CONSUMER ASSISTANCE & INFORMATION

- **Resource for Banking:** Offers insights into protecting your finances, understanding your rights as a consumer, and navigating financial crises with an emphasis on cybersecurity in the banking sector. (https://www.fdic.gov/resources/consumers/)

FBI SCAMS AND SAFETYS

- **Understanding Scams:** Provides details on common scams and crimes, tips on how to protect yourself, and what to do if you become a victim of cybercrime. (https://www.fbi.gov/how-we-can-help-you/scams-and-safety)

As we wrap up this guide, it's important to remember that the landscape of online security is ever-changing, with new challenges and threats emerging regularly. But with the right knowledge, tools, and mindset, you can navigate this landscape safely and confidently.

At Navalign, we're not just committed to managing your financial wealth; we're dedicated to ensuring the security and privacy of your financial life online. We believe in a partnership approach to cybersecurity, where our advanced measures are complemented by your informed actions.

Should you ever have concerns or need assistance with your financial security, our team is here to support you. Together, we can create a secure digital environment, allowing you to focus on achieving your financial goals with peace of mind.