



10.19.26 | FINANCIAL LITERACY

Financial Cybersecurity for Your Entire Family

Michael Davide - Chief Compliance Officer

Protecting your family's financial information starts with everyone—not just the primary account holder. When we think about financial cybersecurity, we often focus on protecting our own bank accounts, investment accounts, and personal information. We create strong passwords, monitor our accounts, and try to recognize suspicious emails. But what about the other members of our household?

The reality is that your family's financial security is only as strong as its most vulnerable connection. A spouse who reuses passwords, a teenager who unknowingly clicks on a malicious link, or an elderly parent who responds to a convincing scam can potentially expose sensitive information and create financial risks for the entire family.

As cybercriminals become more sophisticated, protecting your family's financial well-being requires a broader approach. Financial cybersecurity should be a shared responsibility across generations.

YOUR SPOUSE OR PARTNER: SHARED FINANCES, SHARED RISKS

Many couples share bank accounts, investment accounts, credit cards, and access to important financial documents. However, they may have very different approaches to cybersecurity.

One spouse may be diligent about protecting passwords and identifying suspicious messages, while the other may be less cautious. Because financial information is frequently shared, a security lapse by either person can affect both.

WHAT YOU CAN DO:

- **Use individual login credentials.** Whenever possible, each spouse should maintain separate, authorized login credentials rather than sharing usernames and passwords.
- **Enable multifactor authentication (MFA).** Require an additional verification step when accessing financial accounts, email, and other sensitive services.
- **Review financial activity together.** Periodically review bank and credit card transactions for unfamiliar charges or suspicious activity.
- **Discuss suspicious communications.** Agree to verify unexpected requests involving money or sensitive information, even when the message appears to come from a familiar source.

Having a brief conversation about cybersecurity can help ensure that both spouses understand the risks and follow similar practices.

CHILDREN AND TEENAGERS: A DIFFERENT TYPE OF VULNERABILITY

Children and teenagers are growing up in a digital world. Between social media, gaming platforms, online shopping, and payment applications, they frequently share personal information without fully understanding how it can be used.

Cybercriminals may target younger individuals through fake giveaways, fraudulent online stores, impersonation scams, and messages designed to obtain passwords or payment information.

Children may also unknowingly expose household information through shared devices, email accounts, or saved payment methods.

WHAT YOU CAN DO:

- **Explain the importance of personal information.** Help children understand why they should not share passwords, Social Security numbers, addresses, or financial information online.
- **Review privacy settings.** Ensure social media profiles, gaming accounts, and payment applications have appropriate privacy and security settings.
- **Limit access to stored payment information.** Consider requiring authorization before purchases can be completed.
- **Encourage questions without judgment.** Make sure children feel comfortable telling you if they receive a suspicious message, accidentally click on a questionable link, or believe they have been scammed.

For younger children, parents may also want to consider freezing their credit files as a preventive measure against identity theft.

The goal is not to frighten children about technology, but to help them develop responsible digital habits that will serve them throughout their lives.

ELDERLY PARENTS: RECOGNIZING FINANCIAL SCAMS

Older adults are frequently targeted by financial fraudsters, particularly through telephone calls, text messages, emails, and increasingly sophisticated impersonation scams.

Scammers may pretend to be representatives of banks, government agencies, technology companies, or even family members. Advances in artificial intelligence have made some fraudulent communications more convincing, including the ability to imitate familiar voices.

Common schemes include urgent requests for money, fraudulent investment opportunities, and messages claiming that a financial account has been compromised.

WHAT YOU CAN DO:

- **Have regular conversations about scams.** Discuss common fraud tactics, especially requests that create urgency or pressure someone to act immediately.
- **Establish a verification process.** Encourage elderly family members to hang up and independently contact the organization or person making the request using a trusted phone number.
- **Consider account alerts.** Where appropriate and with their permission, help establish notifications for unusual account activity.
- **Discuss trusted contacts.** Encourage parents to designate a trusted contact with their financial institution who may be contacted if suspicious circumstances arise. A trusted contact does not automatically receive authority to conduct transactions.
- **Create a family verification phrase.** Consider a private phrase or question that family members can use to help verify unusual emergency requests.

Respecting an older family member's independence is important. The objective is to provide support and establish safeguards without unnecessarily restricting their financial autonomy.

SHARED EMAIL ACCOUNTS: AN OVERLOOKED FINANCIAL RISK

Email accounts are often the gateway to our financial lives. Bank statements, investment notifications, password-reset links, tax documents, and other sensitive information may all be delivered through email. If someone gains unauthorized access to an email account, they may be able to reset passwords, impersonate the account owner, or obtain confidential information.

Shared family email accounts can present additional risks, particularly when multiple individuals use the same password or access the account through several devices.

WHAT YOU CAN DO:

- Use separate email accounts for each family member.
- Protect email accounts with strong, unique passwords and multifactor authentication.
- Consider using a dedicated email address for sensitive financial accounts.
- Review account recovery options to ensure unfamiliar phone numbers or email addresses have not been added.
- Avoid sending sensitive financial information through unsecured email.

Protecting your email account is one of the most important steps you can take to protect your financial information.

DEVELOP A FAMILY CYBERSECURITY PLAN

Just as families prepare for emergencies, they should also consider what to do if a financial account is compromised or someone becomes a victim of fraud.

A simple family cybersecurity plan does not need to be complicated. It should identify basic security practices and outline what to do when something suspicious occurs.

FIVE STEPS TO STRENGTHEN YOUR FAMILY'S FINANCIAL CYBERSECURITY:

1. **Review account security.** Ensure financial accounts and important email accounts use strong, unique passwords and multifactor authentication. A reputable password manager can help.
2. **Enable transaction alerts.** Establish notifications for withdrawals, transfers, all credit card activity, and changes to account information.
3. **Consider credit freezes.** Freezing credit files with Equifax, Experian, and TransUnion can help prevent criminals from opening new credit accounts using stolen personal information.
4. **Keep devices updated.** Ensure phones, computers, tablets, and other connected devices receive security updates and are protected by appropriate access controls.
5. **Know whom to contact.** Keep a list of financial institutions and appropriate contact numbers so family members can quickly report suspected fraud or unauthorized activity.

If a family member suspects an account has been compromised, acting quickly is essential. Contact the financial institution through a verified channel, secure affected accounts, and report suspected identity theft to the appropriate authorities.

FINAL THOUGHTS

Protecting your financial well-being involves more than managing investments, saving for retirement, or planning for the future. It also means taking reasonable precautions to safeguard the personal and financial information that supports those goals.

Financial cybersecurity is a family responsibility. By encouraging good security habits, maintaining open communication, and establishing appropriate safeguards, families can reduce their exposure to financial fraud and identity theft.

At Grimes & Company Wealth Management, LLC, we recognize the importance of protecting our clients' financial information. We encourage clients to remain vigilant, discuss cybersecurity with their family members, and contact our team if they receive suspicious communications that appear to involve Grimes or their investment accounts. A few proactive steps today can help protect your family's financial security for years to come.

READ OUR RELATED ARTICLES IN THIS SERIES

- [Protecting Your Financial Accounts: The Trusted Contact](#)
- [Protecting Your Identity: Simple Steps You Can Take Today](#)
- [Protecting Your Wealth: Recognizing and Avoiding Financial Scams](#)

IMPORTANT DISCLOSURES:

This information is provided for general educational and informational purposes only and is not intended as legal, tax, cybersecurity or identity-theft recovery advice. The appropriate steps may vary based on individual circumstances. If you believe you have been the victim of identity theft or fraud, consider contacting the appropriate financial institution, credit bureau, government agency and/or qualified professional promptly.