Keep Your Private Information Private

WHAT IS DIGITAL PRIVACY, AND HOW CAN YOU KEEP YOUR PERSONAL INFORMATION SECURE?

Virtually every interaction – whether online or in real life – involves the exchange of data. Most of the time that exchange is benign, like when we share our name with a new acquaintance or subscribe to a newsletter with an email address. However, when even seemingly harmless information falls into the wrong hands, it can result in incalculable damage to our finances and in our personal lives, be it through stolen credit card numbers, fraud or identity theft.

Data privacy refers to how we can restrict who has access to our personal information and for how long they have it. There are several actions we can take to increase our data privacy while still participating in an increasingly online world.

WHAT YOU CAN DO TO STAY SAFE

The most important thing you can do to keep your personal information secure is to reevaluate your own behavior regarding digital security.

Safeguard Your Personal Information

- Cybercriminals can use personally identifiable information such as a Social Security number, driver's license or medical identification to create a new identity under your name. If you're required to disclose it, ask for the reason behind the request.
- Be mindful of the information you share online, especially on social media. Sharing pictures of your trip mid-vacation could also be announcing that your home is currently unoccupied. Periodically review your social media privacy settings, and try to keep the information you'd need to recover a lost password (like your mother's maiden name) off the internet.
- Use a long and unique easy-to-remember passphrase for each of your accounts. A password manager app can help you create and store strong passwords securely. Use a unique password for each account so that anyone who breaks into one account doesn't have access to all of them. ▶

Wathen Lobel Miller Schultz
Baird
Private Wealth Management
wlmsgroup@rwbaird.com
wlmsgroup.bairdwealth

Keep Your Private Information Private *continued*

- Restrict what your personal devices are sharing about you. It makes sense for a Maps app on your phone to know your location, but if that game you downloaded is also asking for that information, chances are it's looking to sell it to advertisers. Adjust the privacy settings on your devices and browsers to limit what data they have access to. Newer iPhones and iPads offer an App Privacy Report in their settings that can show how you're being profiled and tracked.
- Identity theft services can help you manage your digital footprint and limit the damage from identity thieves. Keeping tabs on your credit history can also alert you to identity theft. You can obtain a free credit report every 12 months by contacting the Annual Credit Report Request Service.

Safeguard Your Documents

- Cybercriminals can use old financial statements and tax documents to steal your identity and commit fraud. Shred sensitive documents you no longer need, including statements and receipts.
- Your physical mailbox can be one-stop shopping for thieves. Put all mail on hold when you're away rather than have it accumulate in your mailbox. If you have outgoing mail containing personal information, like a tax return, drop it off directly at the post office.
- Check your financial statements frequently. If anything looks out of place, contact your banking institutions right away.

Safeguard Your Electronic Communications

- Keep your computer's antivirus software and operating system up-to-date, and install patches for your operating system, applications and web browsers as soon as they're released. Keep out would-be thieves by using a strong password for your Wi-Fi.
- Do not conduct sensitive transactions on a public computer. If you bank or shop on your phone, have the lock screen engage after a short idle time, and be sure to log off instead of just closing a window or browser.
- Similarly, don't conduct important financial transactions using public wireless networks, like those you'd find in airports and cafes – these locations typically lower their security settings to allow for easy public access. If you need to charge your device, plug it directly into an outlet – public USB chargers can be manipulated to upload and download information to and from your device without your knowledge.
- Be skeptical about email asking for personal information – even if you know the sender. One of the first things cybercriminals do upon infiltrating someone's computer is access their address book. If you receive such an email, do not reply, open any attachments or click any links – contact them offline instead.
- Do not send money without verifying all the details.

How Baird Protects Your Personal Information

Keeping our clients' personal information secure is our top priority. That's why we employ a variety of protection strategies to protect your data:

- **We use layered, industry-leading defenses** to protect our most critical systems and client information, including encryption and intrusion prevention systems.
- **We conduct ongoing testing of our critical systems**, including independent reviews conducted by outside security firms, to proactively find vulnerabilities.
- **We require our employees to complete annual training** on information security best practices and security procedures.
- **Our Risk Management department conducts due diligence**, monitors and maintains risk profiles for every third-party organization we work with.
- **We have also partnered with InfoArmor**, an expert in identity theft protection, to offer our clients identity protection and fraud detection services, including financial protection for high-risk transactions, credit monitoring, "dark web" surveillance, digital wallet storage, full-service identity restoration and identity theft insurance. ▶

Keep Your Private Information Private *continued*

Our internal security protocols extend to online access to your accounts. For example, accessing your Baird Online account requires Baird password verification plus multifactor authentication to verify your identity. Every Baird Online transaction is encrypted and transmitted through a secure exchange, and Baird Online accounts automatically log off after a period of inactivity. In addition, our newly redesigned Baird Online mobile app now employs fingerprint and facial recognition so you can log in securely and with ease.

Keeping your personal information private requires a true partnership.

Please reach out if you or anyone you know would benefit from discussing this topic further.