BAIRD
Private Wealth Management

Protecting Your Identity

Tips on keeping your personal information secure, plus what to do if you get hacked

Staying safe in an increasingly online world requires taking measures to keep your personal information out of the hands of cyberthieves. Here are some tips you can use to stay protected.

SAFEGUARD YOUR PERSONAL INFORMATION

- Cybercriminals can use personal information such as a Social Security number, driver's license or medical identification to create a new identity under your name. Do not disclose this information to anyone unless there is legitimate need for it.
- You can have your identity stolen and not realize it for months. An identity theft program can help in managing your digital footprint.

SAFEGUARD YOUR DOCUMENTS

- Cybercriminals can use old financial statements and tax documents to impersonate you or steal your identity. Shred documents you no longer need.
- Your physical mailbox can be one-stop shopping for thieves. Put all mail on hold when you're away and drop off outgoing mail containing personal information directly at the post office.
- Check your financial statements frequently. If anything looks out of place, contact your banking institutions immediately.

SAFEGUARD YOUR ELECTRONIC COMMUNICATIONS

- Keep your computer's anti-virus software and operating system up to date and protect your Wi-Fi with a strong password.
- 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.
- Be skeptical about email asking for personal information – even if you know the sender, as a cybercriminal may have gotten hold of their email address book. If you receive such an email, do not reply, open any attachments or click any links. Verify offline instead.
- Do not send money without verifying all the details.

Tips for Creating a Strong Password

- Create a password that is easy to remember but hard to guess.
- If you store passwords in a file on your computer, encrypt the file and assign it a strong password.
- Create a unique password for each account so that thieves who break into one account don't have access to all of them.

WHAT TO DO IF YOU ARE HACKED

There is no quick fix to restoring your identity if you've been hacked – but you may be able to limit the damage done by acting quickly.

COMPLETE A FRAUD ALERT

Your credit file is tracked and monitored at three credit bureaus: Equifax, Experian and TransUnion. By filing a fraud alert with all three, any request to access your credit will immediately be flagged. While fraud alerts typically expire in 90 days, victims of identity theft can file for an extended alert lasting seven years.

MONITOR YOUR CREDIT

Unsure if your personal information may have been compromised? You can monitor your credit through reputable credit monitoring service firms.

FREEZE YOUR CREDIT

A credit freeze is a total lockdown of new account activity in your name – once frozen, no account transactions can be processed or new accounts opened until the credit account is "unfrozen." To learn more about credit freeze laws in your state, visit consumersunion.org.

CONTACT THE IRS

One way cyberthieves profit from identity theft is through filing a bogus tax return and claiming a fraudulent refund. To learn more, download the IRS' "Taxpayer Guide to Identity Theft" at irs.gov.

SECURING YOUR PERSONAL INFORMATION

At Baird, we take your security needs very seriously. Accessing your Baird Online account requires Baird password verification and multifactor authentication that verify the user's authenticity. Any transaction through Baird Online is also encrypted and transmitted through a secure exchange, and Baird Online account automatically logs off after a period of inactivity.

BAIRD'S PARTNERSHIP WITH INFOARMOR

Baird has partnered with InfoArmor, an expert in identity theft protection, to provide our clients with identity protection and fraud detection services. This service is available for $9.95/individual and $17.95/family per month for Baird clients – a significant discount from standard rates.

InfoArmor's identity theft protection includes the following services:

- Financial protection for high-risk transactions
- Credit monitoring, monthly credit scores and an annual credit report
- "Dark web" internet surveillance
- Digital wallet storage
- Lost wallet protection
- InfoArmor's social media monitoring

Your identity protection coverage provided by InfoArmor through Baird also includes full-service identity restoration and $1 million in identity theft insurance. Please contact your Baird Financial Advisor for enrollment details.

ADDITIONAL RESOURCES REPORTING CYBERCRIME

- You can report internet fraud to the FBI by calling 202-324-3000 or ic3.gov.
- To contact the Federal Trade Commission about identity theft, call 877-438-4338.
- To contact the Postal Inspection Service, call 877-876-2455.
- To contact the IRS, call 800-829-0433.
- To contact the Social Security Administration, call 800-269-0271.
- To remove your name from telephone marketing lists, visit donotcall.gov.
- https://www.equifax.com 1-888-378-4329
- https://www.experian.com 1-888-397-3742
- https://www.transunion.com 1-833-806-1627