Protecting Yourself From Electronic Identity Theft

Protecting client information is a top priority at Baird, and we employ a variety of security measures to safeguard your accounts on top of regular, ongoing monitoring. However, for identity protection to be truly effective, you have a part to play. This guide offers steps you can take to protect your identity and sensitive information from online thieves.

What If Your Email or Social Media Account Has Been Hacked?

Update your system and delete any malware

If you don't have security software, get it – but install security software only from reputable, well-known companies.

Set your security software, Internet browser and operating system (like Windows or Mac OS) to update automatically

Keep your security software, your Internet browser, and your operating system up-to-date to help your computer keep pace with the latest hack attacks.

Change your passwords

If you use similar passwords for other accounts, consider changing them. Tips for creating effective passwords can be found on the next page.

Contact your email provider or social networking site about restoring your account

Contact your email provider or social networking site for assistance.

Notify your financial institutions

You will need to contact every financial institution where you hold accounts to ensure your finances are in safekeeping.

Reach out to your credit reporting bureau

Ensure you have reported the incident and that the bureau knows about your situation.

Contact your local police

If someone has stolen your identity, contact your local police to file a report.

continued

Check your account settings
Once you're back in your account, make sure your signature and "away" message don't contain unfamiliar links, and that messages aren't being forwarded to someone else's address.

Tell your friends
A quick email letting your friends know they might have gotten a malicious link or a fake plea for help can keep them from sending money they won't get back or installing malware on their computers.

More resources
Please refer to these resources for additional information on identity theft.

http://www.consumer.ftc.gov/features/feature-0014-identity-theft

http://www.finra.org/Investors/ProtectYourself/AvoidInvestmentFraud/ProtectYourIdentity/

How You Can Protect Yourself from Identity Theft

Create multiple, unpredictable passwords
A password only works if a would-be thief can't figure out what it is. Here are some password creation tips to help keep identity thieves at bay:

- The longer the password, the tougher it is to crack. Ideally, 12 characters for most home users.
- Mix letters, numbers, and special characters.
- Try to be unpredictable – don't use your name, birth date or common words.
- Don't use the same password for multiple accounts.
- Don't share passwords on the phone, in texts or by email. Legitimate companies will not send you messages asking for your password.
- Periodically change your password.

Safeguard your user names, passwords and other personal information
Never provide credentials like user names and passwords in response to an email. If the email or text seems to be from your bank, visit links and access telephone numbers from the bank website.

Don't open email attachments or click on links without knowing what they are
That link or attachment – even in emails that seem to be from friends or family – could install malware on your computer.

Treat your personal information like cash
"Phishing" is a technique used by scam artists, posing as legitimate companies to try to convince you to divulge personal financial information such as passwords and account numbers. Practice great caution if you ever receive an email asking you to disclose personal information.

Give personal information over encrypted websites only
If you're shopping or banking online, stick to sites that use encryption to protect your information as it travels from your computer to their server.

If you reach a website that appears to be a fraudulent Baird site or are ever in doubt of our site's integrity, please contact Baird directly by calling 888-212-8843.

Download software only from sites you know and trust
If you're not sure whom to trust, do some research before you download any software.

Use different email addresses for different purposes
Should someone hack into an email address, his or her access would be limited to that one account.

Be careful when using public Wi-Fi
Public Wi-Fi is just that – public. Don't transmit information you wouldn't be comfortable with other people knowing.

Avoid leaving personal information on your computer screen
It's not nearly as high tech, but it only takes a few seconds for someone to copy down account and credit card numbers from an unguarded screen.