Protecting Your Identity, Data, and Assets
It’s Not a Matter of If, but When…

17.6 million people experienced identity theft in 2014

63% of confirmed data breaches involved weak, default, or stolen passwords

Identity fraud is a serious issue. Fraudsters have stolen $112 billion in the past six years, equating to $35,600 stolen per minute

Source: Bureau of Justice Statistics
Source: Verizon 2016 Data Breach Investigations Report
Source: 2016 Javelin Strategy & Research, Survey Report Results
Identity Theft is Everyone’s Problem

- **Identity theft is the fastest growing crime in America.**
  
  **Source:** Trans Union Website, January 14, 2015

- **Someone’s identity is stolen every 2-3 seconds.**
  
  **Source:** https://identity.utexas.edu/id-perspectives/top-10-myths-about-identity-theft

- **The average loss per identity theft incident is $4,930.**
  
  **Source:** U.S. Department of Justice, Javelin Strategy & Research

- **On average it takes 600 hours to recover from identity theft.**
  
  **Source:** The Identity Theft Resource Center website, April 28, 2015
Discussion Topics

• Common cyber threats
• Protecting your data
  – How we protect your data
  – How you can protect your identity
    ▪ Dos and Don’ts for protecting your data
• Other helpful resources
Common Cyber Threats

1. E-mail Hacking
2. Malware
3. Phishing
4. Spoofing
Email Hacking

**What does it look like?**
A cybercriminal gains access to your email (often by figuring out your password) and then, posing as you, emails your advisor or family members instructions to forward funds to an account they control.

**What’s the impact?**
Because the cybercriminal has access to your email and can impersonate you, the recipient of the cybercriminal’s email believes the correspondence comes from you. The cybercriminal may provide instructions within the email to transfer funds to a fraudulent account. Without proper verification, the money could be transferred and stolen.

Malware

**What does it look like?**
Examples of malware include malicious programs like viruses, worms, trojan horses, ransomware, and spyware.

**What’s the impact?**
Malware can delete files or directory information, or it may allow attackers to covertly gather personal data, including financial information and usernames and passwords. It can also be used to lock your electronic devices allowing them to ransom your own data back to you.
Phishing

What does it look like?
An email from a seemingly legitimate email address instructs you to click on a link to take action (e.g., “validate your account,” “confirm your identity,” “access your tax refund”). The link brings you to a website requiring you to enter your personal information.

What’s the impact?
Victims of phishing may have malware installed on their computer systems or, by entering their user credentials into a system controlled by a hacker, have their identity or financial information stolen.

Spoofing

What does it look like?
A fake email header that gives the impression the email is from someone or somewhere other than the actual source, with the goal of tricking the recipient into opening and responding to the email.

What’s the impact?
Similar to the other cyberattacks we’ve discussed, your money is stolen, and you inadvertently provide your user credentials or personal information to a criminal, enabling them to access your funds or use your identity.
# How We Protect Your Personal Information and Assets

<table>
<thead>
<tr>
<th><strong>Cybersecurity program</strong></th>
<th>Blankinship &amp; Foster’s Cybersecurity program is designed to ensure the security and confidentiality of our clients’ personal information. Our staff adhere to our Cybersecurity Policies and Procedures in order to protect against unauthorized access to our computers, networks and communications.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Staff and vendor vetting</strong></td>
<td>We vet staff and vendors before allowing any access to our clients’ personal information. Our staff vetting includes background checks, reference checking, and checks of credit reports and criminal databases.</td>
</tr>
<tr>
<td><strong>Staff training</strong></td>
<td>Blankinship &amp; Foster regularly trains our staff on privacy, data protection and cybersecurity. We also ensure that our vendors maintain effective cybersecurity programs and trained on them.</td>
</tr>
<tr>
<td><strong>Systems and Equipment</strong></td>
<td>We invest in strong protections such as firewalls, data encryption, and secure systems to transmit information.</td>
</tr>
<tr>
<td><strong>Authentications and funds transfer policies</strong></td>
<td>Before executing any requests to transfer funds, we always authenticate our client’s identity and the instructions.</td>
</tr>
</tbody>
</table>
How You Can Protect Your Data
Ways You Can Protect Your Data

- Be strategic with usernames and passwords
- Keep your equipment up to date
- Safeguard email accounts
- Surf safely
- Protect your money
- Limit what you share online
Be Strategic With Usernames/Passwords

**Do**

- Create passwords that are long and strong, using 12-16 characters, upper- and lowercase letters, numbers, and symbols.
- Use a unique password for each account to prevent a quick and invasive attack on all of your accounts, known as credential replay.
- Where available, use two-factor authentication when accessing your accounts.

**Don’t**

- Use information that can be easily found about you online or otherwise.
- Share passwords with others.
- Use any part of your Social Security number, birth date, or other personal data when creating passwords.
Surf Safely

**Do**

- Use wireless networks you trust and know are protected.
- Be cautious when using public computers.
- Ensure you are downloading legitimate apps from trusted publishers.
- Be aware that secure websites start with https, not http.
- Be sure to log out completely (which terminates access) when exiting all websites to prevent cybercriminals from obtaining your personal information.
- Consider purchasing a personal Wi-Fi hot spot.
- Hover over questionable links to reveal the true destination before clicking.

**Don’t**

- Use public computers or public WiFi (like airports or coffee shops) to access confidential information or accounts, or to perform financial transactions.
- Click on websites you don’t know or on pop-up ads or banners.
Protect Your Money

**Do**

- Review your credit card, cell phone, and financial statements as soon as they are available, or more frequently online.
- Contact your financial institution if you see anything suspicious on your statements.
- Help us protect your information and assets by following our guidelines for identification verification and procedures for transferring funds.
- Opt for voice authentication as an added layer of protection when available.

**Don’t**

- Send your personal identifiable information or account information via unsecure channels like email, chat, or text.
- Respond to requests for personal information from an unsolicited email or from an unsolicited incoming phone call.
Limit What Your Share Online

Do

• Be very selective about the information you choose to share on social media and with whom you choose to share it.

• Keep your personal information private (home address, phone number, and birthdate).

• Set privacy and security settings on web services and devices to your comfort level for sharing.

Don’t

• Post personal information about family and friends online.

• Accept friend requests on social media from people you don’t personally know. Many hackers use social media to learn details like birthdays, address and pet names.
Do

- Exercise caution when reviewing unsolicited email.
- Obtain secure storage programs to archive sensitive, private data, and documents instead of storing emails.
- Create separate email accounts specifically for financial transactions.
- Delete all emails that include financial information.
- Cautiously evaluate the risk versus convenience of transferring confidential information by email.

Don’t

- Do not click on the links or pop-up ads in unsolicited emails, as these links may pass on viruses.
Keep Equipment Up to Date

<table>
<thead>
<tr>
<th>Do</th>
<th>Don’t</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Install the most up-to-date antivirus and anti-spyware software on all devices that connect to the Internet (e.g., PCs, laptops, tablets, smartphones)</td>
<td>• Don’t purchase any networking devices secondhand.</td>
</tr>
<tr>
<td>• Set each device to run regular scans to update software.</td>
<td>• Forget to set up a passcode or PIN and auto-lock on your mobile devices.</td>
</tr>
<tr>
<td>• Ensure you’ve installed the latest versions of your software and your patches are up to date.</td>
<td>• Forget to change the factory default passwords on home electronic devices, especially routers and other devices connected to the web like smart TVs.</td>
</tr>
<tr>
<td>• Make sure your networking equipment and computers are all still supported by the manufacturer.</td>
<td>• Use free or found USB drives, as they typically are infected with malware.</td>
</tr>
<tr>
<td>• Recycle, exchange, or dispose of your old mobile device safely.</td>
<td></td>
</tr>
</tbody>
</table>
Additional Resources

Industry Resources:

• Go to StaySafeOnline.org and review the STOP. THINK. CONNECT.™ cybersecurity educational campaign

• Visit OnGuardOnline.gov, also a part of the STOP.THINK. CONNECT.™ campaign, that focuses on online security for kids and includes a blog on current cyber trends

• Visit https://www.fbi.gov/scams-safety/fraud to learn more about common fraud schemes

• Go to Schwabsafe www.schwab.com//schwabsafe to learn about Schwab’s security measures.

• Go to https://howsecureismypassword.net/ to check your password strength

To Report a Cybercrime:

• Forward suspicious emails to: nophishing@cbbb.bbb.org

• Visit www.identitytheft.gov to report identity theft and to get a recovery plan

• Go to FTC.gov for additional consumer resources and to report identity theft

• http://www.ic3.gov/default.aspx is another website where you can file cybercrime complaints