

We've set out below a number of actions you can take to reduce the chance of being a victim of a cyber-attack.


### **TIPS FOR PERSONAL CYBER SECURITY**

1. **Freeze your credit: THIS IS OUR #1 TIP.** Credit freezing is one of the most effective tools against identity theft. Freezing stops identity thieves from applying for credit under your name using info they stole from you. This is not the same as credit monitoring, which just lets you know that someone may be using your identity. The cost of freezing your credit is minimal. It's easy to "thaw" your credit files when needed. Don't freeze if you often create new accounts with financial institutions or if your credit reports are often accessed for work. See <http://www.clarkhoward.com/credit-freeze-and-thaw-guide> for more information and for links to the websites for three credit agencies.
2. **Look at email addresses before clicking on a link:** Spoofing and phishing rely on your not looking closely at who is sending the email. Hover on suspicious email addresses or links to see if the sender is legitimate. E.g., if the sender's email address is off by even one letter (e.g., bllaw.com rather than blaw.com), it is likely bad. Don't open links or docs unless you can be sure of the sender. Even if the sender is a friend asking you to open a file or click on a link, be very suspicious. Many cyberattacks are launched by hijacking someone's email account and sending emails from a legitimate email (your friend's), but with the malware in an attached file or link.
3. **New: Hovering over an email address:** Hovering over an email address to see if it is legitimate is no longer completely effective because this can be faked. But, replying (but not sending the reply) will show the true email address that the reply would go to.
4. **Use passphrases, not passwords:**
  - a. Don't use passwords; use passphrases, [e.g., Benplays643b@seball] (with upper/lower case and symbols) plus numbers (e.g., 3 digits in the middle) that you can change easily.
  - b. Change your passphrase occasionally. Create a pattern for your change to make it easier. For example, change the number in the middle of the passphrase.
  - c. Use different passphrases for junk and for financial —if one is hacked, the other isn't.
  - d. If you suspect bad activity on your personal email account, log out, change the password, and go into the Rules area of the settings panel to see if the hacker created a rule to automatically forward your emails to the hacker.
5. **Change Wi-Fi router and other connected devices password:** Change your home Wi-Fi router password occasionally. Make sure it is not the default one from when you installed it. Change your Wi-Fi router's setting to disable broadcasting the network name. Same with wireless door locks, security systems, etc. Don't name your router in a way that can identify you or your location. Put internet-connected devices on a separate Wi-Fi network.
6. **Use "two-factor authentication" for online storage:** For online storage services like Dropbox, Box, OneDrive, GoogleDrive, etc., use two-factor authentication to raise the

security level. Two factor authentication involves “something you know” (the first factor, e.g., password) and “something you have” (the second factor, one-time passcode generated by your phone). The “something you have” is often a one-time verification code that’s sent to your smartphone via SMS, via an app (e.g., Google Authenticator, which is free), or by biometric authentication (e.g., fingerprint).

7. **Know your data:** Know what types of data you have (healthcare, tax, financial, photos, music, documents) and protect sensitive data more securely.
8. **Backup routinely, and offline:**
  - a. Storage space is cheap.
  - b. Backup to a separate drive. Don’t backup your Quicken file to the computer the software is on.
  - c. Ransomware can attack ***every*** storage device connected to your home network or computer, not just the computer initially infected. Disconnect your external backup drives from the internet and from your computer or home network to avoid ransomware locking up your backup drives. Use two backup drives and keep one of them offline until needed. Photos and music usually don’t change very frequently, so keep an extra copy offline.
9. **Don’t use unknown flash drives:**
  - a. Don’t insert a flash drive into your computer unless you are certain where it came from. Malware can be on the flash drive and merely inserting it into your computer will result in the virus being uploaded.
  - b. Encrypt your flash drive (e.g., with BitLocker) before storing confidential files on it so that if it is lost, files won’t be readable. Label that flash drive with an E (e.g., with a Sharpie or White-Out) to note that it is encrypted.
10. **Think before using public Wi-Fi for sensitive transmissions:** don’t use it for transmitting sensitive data.
11. **Update and patch software regularly:** Install operating software and firmware (e.g., router) patches and updates as soon as they are sent out. Set your computer to either automatically download and install updates weekly, or to alert you to do so. You can’t be protected against new threats if you don’t install security updates promptly. Hackers check the available databases of new patches daily for patches fixing specific security holes---and then immediately go out and try to exploit the newly-discovered (and announced!) hole before companies apply the patch.
12. **Use secure websites for credit card transactions:** Before submitting credit card information online, look at the URL and make sure it starts with **https**, which means it is a secure site, rather than **http**.
13. **Create false answers to “security challenge questions”:** Many financial-related websites ask you to verify your identity by answering personal questions. Remember that the answers need to be ones you can remember, they do **NOT** need to be accurate or truthful. Use fake answers. It is very easy for hackers to learn your home town, elementary school, maiden name, etc., from social media.

14. **Personal email accounts:** Add your own email address to your contacts. If your account is hacked and used to send emails to your contact list, you will get an email from your own account, which can tip you off. Change your password at least every 6 months. If you get similar emails from your friends, alert them that their account may have been hacked.
15. **Get an IRS PIN:** If you live in GA, FL, or DC, or, regardless where you live, if you have been the victim of identity theft, get an Identity Protection PIN number from the Internal Revenue Service to prevent a fraudster from filing a false tax return using your name and information. The website for more information is <https://www.irs.gov/identity-theft-fraud-scams/the-identity-protection-pin-ip-pin>.
16. **Use different web browsers:** Use one browser (e.g., Chrome, Safari, Firefox, Internet Explorer) for casual web browsing, and a different one for financial transactions. If your casual browsing leads to giving up cookies, your transaction information won't be compromised.
17. **Manage your digital estate:** Make sure your will has documentation to be able to show online service providers who has the authority to take control of your accounts after you die. A "digital executor" can be assigned to be responsible for disposing (e.g., shutting down, transferring or maintaining) of your email and social media accounts. Keep an offline journal of your key online accounts (e.g., banking, online bill pay, medical) and how to access them. Keep your important documents on an external hard drive, which may be easier for your digital executor to access than the cloud storage providers if you don't provide a password.
18. **Don't allow "persistent access" to your contacts or emails:** Close out of web-based email sessions (e.g., Yahoo, Gmail, Outlook) and other accounts when done to prevent a hacker from accessing your emails without a password.
19. **Prevent "skimming" of your credit card:** Use the gas pumps near the cashier. They're less likely to have had a device attached that can acquire your credit card info.
20. **Stop a fraudulent wire transfer:** Call the FBI within 24-48 hours after a potentially fraudulent wire transfer is made. Their Financial Fraud Kill Chain may be able to stop the next transfer and recover your money.

	
<p><b>Jason A. Bernstein</b>          Phone: (404) 264-4040  <a href="mailto:jason.bernstein@btlaw.com">jason.bernstein@btlaw.com</a></p>	<p>Partner</p> <ul style="list-style-type: none"> <li>➤ Data Security &amp; Privacy (Group Co-Chair)</li> <li>➤ Technology Agreements</li> <li>➤ Intellectual Property</li> </ul>
<p>Barnes &amp; Thornburg LLP          3340 Peachtree Road, N.E.          Suite 20900          Atlanta, Georgia 30326  <a href="http://www.btlaw.com">www.btlaw.com</a></p>	