https://stoutbowman.com/hackproof.html

**Hack-Proof Your Life**

The New Cybersecurity Rules You Must Follow To Prevent Identity Theft

## The following information comes from the book

*Hack-Proof Your Life Now! (https://www.amazon.com/Hack-Proof-Your-Life-Cybersecurity-Rules/dp/0997729007)* by Sean M. Bailey and Devin Kropp. We highly recommend that you consider purchasing this book. Stout Bowman & Associates has no affiliation with Mr. Bailey, Mr. Kropp or their publisher.

Just how hard is it for someone to hack into your life and steal your identity? Let's look at a case study:

Starting with just a name, hometown and employer, the hacker Googled her name and discovered an old resume and a personal blog. The resume included her old college email address, and the blog her personal email address.

Bringing up the school's email login page, the hacker used the “reset password” feature, which asked for the user's birth date. Having discussed her birthday on her blog, the hacker made his first penetration — he now had access to one his target's email addresses.

In order to gain access to her personal email, the hacker then did the same email password reset function on her personal email account, using information gleaned from her resume and blog to answer the security questions. The email provider then sent the password reset email to her secondary account — the school account that he now controlled.

Now that he had control of her personal email account, it was easy to access her bank's online service (using information about where she lived and what banks with which she might have an account) and, once again, answer the security questions of the

password reset function using information from her resume and blog. Since he now controlled the target's personal email account, and the password reset link was sent to her personal email, he could change the bank account access password and now had control of her account. Also, with access to her email account, the hacker could easily discover other financial accounts used by the target, such as PayPal, Amazon, eBay, credit cards, etc.

Thus, by finding out one critical piece of information, the school email account, the hacker was able to ultimately gain control of the target's bank account. There are many other critical elements of our digital identity that can have a similar domino effect and result in a severe cybersecurity breach.

## Now for the things you MUST do to protect yourself from identity theft

The following can be viewed as a checklist; for a more detailed explanation on how to accomplish each item, you will need to refer to the book, or, if you are a client of Stout Bowman, you may use our *contact form* and we'll give you a call back to help you through this process.

1. Create a **secret email address** for your financial accounts, and set it up with the strongest possible security settings. For example, do not use all or part of your name as the user name (the part before the @ sign), and use a phone password recovery function instead of security questions.

2. Always use a **strong password**, utilizing letters, numbers and symbols. A mnemonic is good, a goal-setting phrase better, and unbreakable passphrases and poetry best.

3. Utilize **two-step verification** for your financial accounts whenever available. By using two steps, one a login password and the other a phone call or text from the financial institution, requires two separate things — something you know (the password), and something you have in front of you (your phone).

4. Get and use a **password manager**. Coming up with many different and complex password is a pain, and leads one to defer to “normal” security due to password fatigue. A password manager, such as Lastpass or Dashlane, means you only need to remember one password, that of the password manager.

5. Be very cautious when using free public WiFi; consider using a **Virtual Private Network (VPN)** service. Since hackers can easily monitor the traffic on an unsecured WiFi network, never use it to access anything that requires login credentials. A VPN software program establishes its own encrypted connection to the Internet. Another secure option is to use your **phone's WiFi hotspot app** to provide a secure connection.

6. Secure your **home WiFi network**. In short, a) change your router's default username and password, b) encrypt your router, c) disable WiFi Protected Setup (WPS), and d) update the router's software.

7. Add **passcodes** to your devices, activate the Find my iPhone or Locate My Phone app, and add your emergency contact information.

8. Review and strengthen your **privacy settings** on social media, and reexamine your “friends” to ensure you're still comfortable sharing with them.

9. Put **alerts on your bank and credit cards**. For many accounts, the sooner you report fraud, the less liability you have for the fraudulent charges.

10. **Freeze your credit files** with all three reporting agencies: Equifax, Experian and TransUnion. While most offer two other lower security settings, Credit Monitoring and Fraud Alert, they don't provide the strong, lasting protection you need to prevent identity theft.

11. **Protect your child's identity**. Request a search of your children's Social Security numbers with all three credit agencies, and review your state's laws to determine the best way to protect your children from identity theft.

12. Watch for **skimming devices**. Avoid using non-bank ATMs for withdrawing cash, and understand how to spot skimmers on any ATM or payment kiosk.

13. Install and update **antivirus software** on your computers and devices.

14. Always **update your software** when prompted, and set up to download automatically any future updates. Uninstall or disable unsafe programs.

15. Back up ALL your data on ALL you devices so you never pay **ransomware extortions**. Back up to two different locations; the cloud and a physical device.

16. **Examine messages for signs of fraud**. Learn how to unmask an email's true sender, and understand how to examine an email message for the key signs of fraud.

17. **Inspect links to confirm fraud**. Know how to examine links in suspicious emails to determine if they're real or fraudulent. Recognize the danger of opening any unsolicited email attachment.

18. Take control of your cybersecurity now. Identity monitoring companies don't offer you the strongest protection — the Security Freeze (see item 10). **You're the best person to protect your identity — at practically no cost**.

Note: Stout Bowman & Associates is NOT a cybersecurity firm. We are providing this information to encourage our clients to take cybersecurity threats seriously and provide them with recommendations from what we believe to be competent authorities on the subject.


555 Gettysburg Pike Suite C-100, Mechanicsburg, PA 17055
717-761-2040