Savvy Cybersecurity™ Quick Reference Guide, 2015

Jim Rees, CRPC
President/Financial Advisor
Stoneway Financial., LLC.
5080 Spectrum DR
Ste 1000E
Addison, TX 75001
972-447-5170
Jim@stonewayfinancial.com
www.stonewayfinancial.com

A. Scorecard

Answer Yes or No to the following questions. When complete, follow directions at bottom to get your raw score and rating. Then review checklist and complete action plan.

Topic	Question	Yes/No	Score
CREDIT REPORTS:	I know the difference between putting my credit files on monitor, alert, or freeze AND I've had my minor children's names searched at the credit bureaus.		15 pts
SOCIAL MEDIA:	I have reviewed my "privacy settings" that control who sees and reads what I do on Facebook and other social media sites.		5 pts
COMPUTER/ LAPTOP:	My personal computers have the most updated operating systems, browsers, virus/malware/firewall software, and up-to-date versions of Java, Flash, and Adobe.		10 pts
BUSINESS ID THEFT:	My employer trains its staff on business or personal cybersecurity measures.		5 pts
WI-FI:	I know how to determine if FREE public Wi-FI is safe to use.		10 pts
DEVICES:	My smartphone and/or tablet has a security passcode.		5 pts
PASSWORDS:	I have enabled two-factor authentication on my key accounts that allow it.		15 pts
SKIMMING:	When using an ATM card, or self-paying for things such as gas, tickets, parking, I know what to look for to ensure that my transaction is safe from being fraudulently recorded.		5 pts
DATA BREACH:	I have text and email alerts set up on my credit cards and bank accounts to receive a notification each time there is a transaction.		15 pts
PHISHING:	I know the tactics used by phishers to try to trick me into clicking on links or sharing personal information.		15 pts
Circle points for each question answered with a Yes. Add points to get score. Consult section B to get your cybsersecurity rating.		Raw Score:	

B. Rating

>100-85	**GOOD**
84-60	**OKAY**
59-0	**DANGER**

Consult the Checklist in section C to identify key items to include in your Action Plan in section D.

C. Checklist

✓	Action	Time	Points
	Principle #1: Devices		
☐	Create a passcode for smartphone and tablet.	2 min	4 pts
☐	Install "Locate My Device" or "Find My Phone" app in case device is lost or stolen.	1 min	1 pt
	Principle #2: Software		
☐	Update all software on your home laptop/computer.	5 min	10 pts
	Principle #3: Wi-Fi		
☐	Secure home Wi-Fi network by changing default password and name.	20 min	10 pts
	Principle #4: Passwords		
☐	Change weak passwords to strong and secure passwords.	5 min	2 pts
☐	Passwords don't include names, birthdates, pets' names, etc.	Always	1 pt
☐	Passwords include nonconsecutive numbers and symbols.	Always	1 pt
☐	Keep passwords unque and change every six months.	Always	1 pt
☐	Use a mnemonic device to create password.	5 min	3 pts
☐	Enable two-factor authentication on accounts that allow it.	Always	5 pts
	Principle #5: Transactions		
☐	Sign up for text/email alerts for debit/credit cards.	2 min	10 pts
	Principle #6: Credit		
☐	Sign up for credit freeze.	20 min	15 pts
	Principle #7: E.M.A.I.L.		
☐	Examine messages and inspect links before clicking.	Always	15 pts
	Additional Cybersecurity Actions		
	Document Safe		
☐	Put personal documents in a safe place.	2 min	1 pt
☐	Shred documents with personal information with a cross-cut shredder before throwing them out.	1 min	2 pts
☐	Give out Social Security number only when necessary. Question why.	Always	2 pts
	Social Media Safe		
☐	Strengthen Facebook and other social media privacy settings.	5 min	2 pts

Check with your financial advisor for updates.

Checklist (cont.)

Credit Safe			
☐	Request and review copy of credit report.	30 min	5 pts
☐	Request search on child's Social Security number at all three credit bureaus.	1 hour	5 pts
Wallet Safe			
☐	Remove blank checks from wallet.	1 min	1 pt
☐	Remove Social Security card from wallet.	1 min	1 pt
☐	Remove written PINs or passwords from wallet.	1 min	1 pt
Bank Safe			
☐	Check bank and credit statements regularly.	5 min	2 pts
☐	Switch to online banking.	5 min	1 pt
Medical Safe			
☐	Review all health insurance statements for false claims.	Always	5 pts
Business Safe			
☐	Put 2-factor authentication on bank wire transfers.	Always	5 pts
☐	Check security on company/ corporate registrations at state level.	10 min	2 pts
☐	Limit dollar amount of unauthorized wire transfers.	10 min	2 pts
☐	Implement ID Theft training for employees.	Always	2 pts
☐	Register all domain variations of your website.	20 min	1 pt
ATM Safe			
☐	Use only bank ATMs.	Always	3 pts
☐	Inspect ATM for skimming device at door entry and before using machine.	1 min	3 pts

D. Action Plan

I commit to taking the following steps to boost my cybersecurity by this date: ____/____/____

❶	
❷	
❸	

Signature:

Password Letter to Symbol Conversion Chart

Change this...	To this...	Example phrases made into passwords	
At	@	Run everyday	Run3v3ryd@y
For	4	Eat more fruit	3@t>fru1t
To, Too, Two	2	Sleep at 11	$l33p@11pm
S	$	Bring own lunch	Br!ng0wnlunch!
I	1 or !	No more soda	N0m0r3s0d@
E	3	Save for house	$@v34h0u$3
A	4 or @	Get outside	G3t@0ut$!d3
O	0		
And	&		

Resources

United States

Credit Reporting Agencies:
Experian: 800-525-6285
Equifax: 800-846-5279
TransUnion: 877-322-8228

FTC:
877-438-4338

Canada

Credit Reporting Agencies
Equifax Canada: 866-828-5961
TransUnion Canada: 800-663-9980
Quebec Residents: 877-713-3393

Canadian Anti-Fraud Centre:
1-888-495-8501

Computer Hack Response Guide

1. Run an anti-virus scan of your computer.
2. Change password of affected account and any account with the same password. It is a good idea to change all passwords at this time.
3. Update all software on your computer/laptop/device.
4. Contact your credit card company/bank. Alert them of the fraud and ask to close affected accounts and open new ones with new cards.
5. Contact one of the big three credit reporting bureaus and place a fraud alert on your credit. This will make it harder for a thief to obtain new credit in your name. You only need to alert one bureau; they will alert the other two. Consider placing a credit freeze.
6. Order a copy of your credit report from the three credit reporting bureaus. Review your credit report and dispute fraudulent activity.
7. File a police report.
8. Submit an Identity Theft Report to the FTC. Visit their website for instructions.
9. Close any other accounts that you believe may be affected.
10. Continue to monitor all financial accounts for any fraudulent charges.