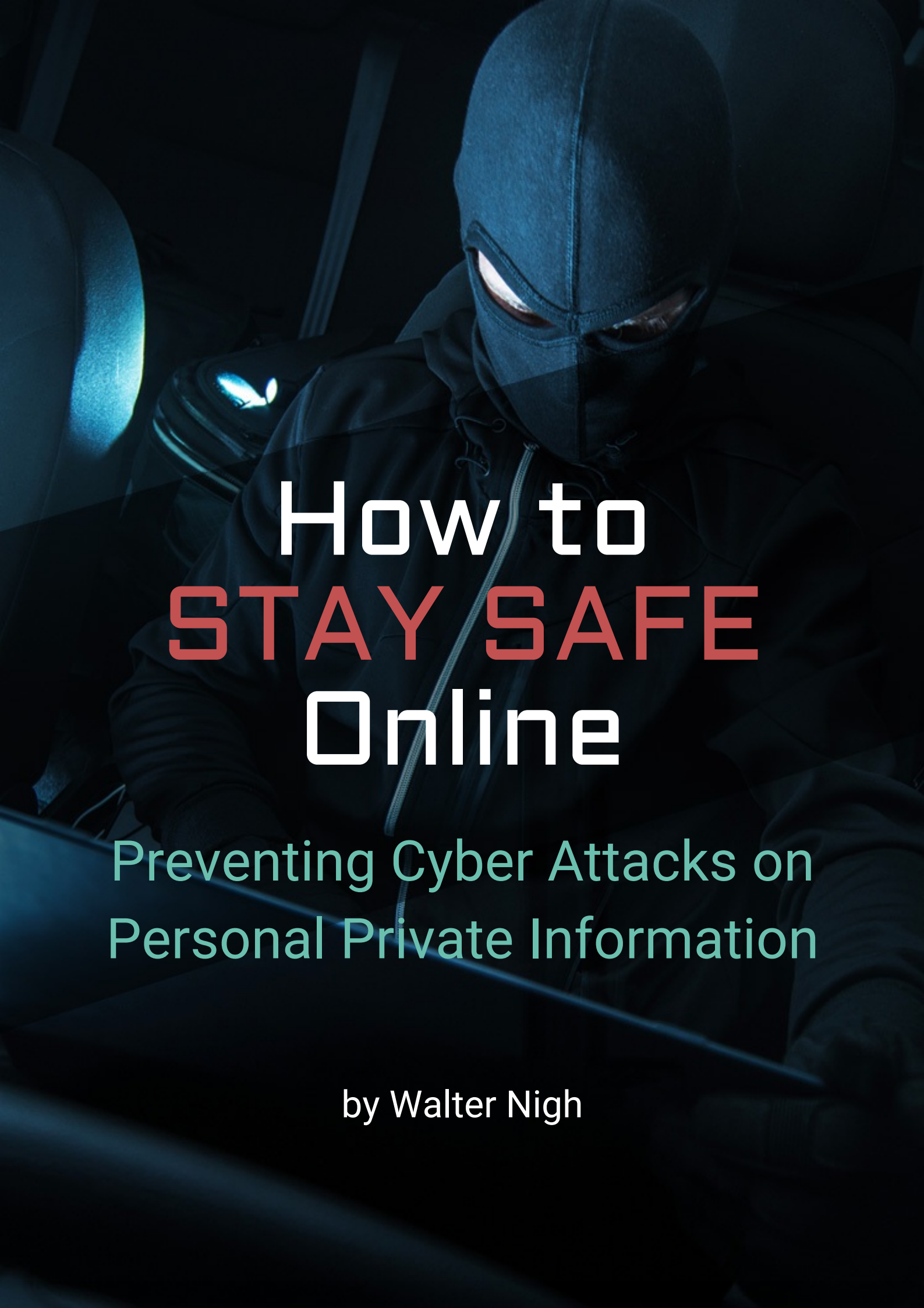


How to STAY SAFE Online

Preventing Cyber Attacks on Personal Private Information

by Walter Nigh

Our daily lives are rapidly centering around online shopping, online banking, online gaming and other online business adventures.

Navigating the minefield of the internet can be dangerous, frustrating and expensive – especially if you have fallen victim to an online scam or your private and personal information has been hacked.

In 2017, the FBI (Federal Bureau of Investigation, USA) received more than 300,000 complaints of criminal internet activity with more than $1.4 Billion in reported losses.

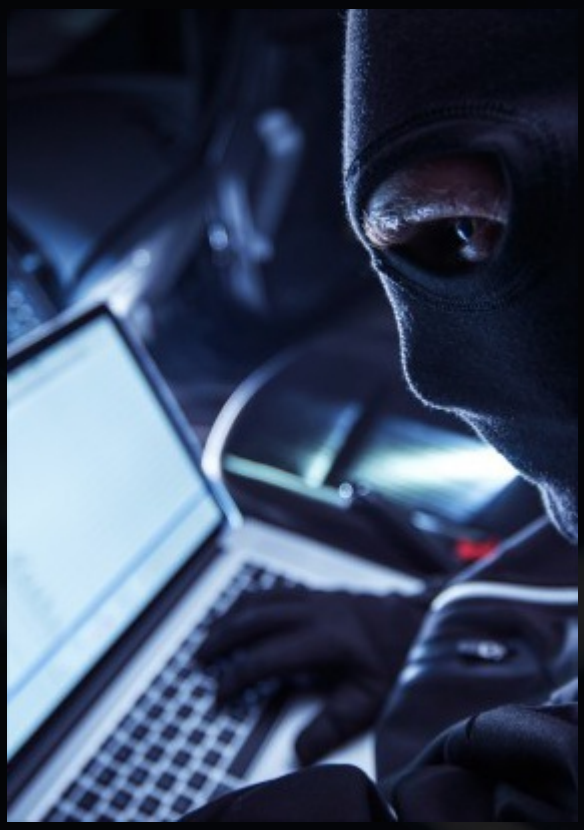
That's "B" for BILLION! No small potatoes and a huge loss for many unsuspecting online citizens.

Many unsuspecting internet denizens are being swindled and scamboozled by skilled and devious marketers seeking to shortcut their way to online riches and take everything, or as much as they can, from you.

Always be on the lookout to protect your personal information like it's pure gold – because to hackers and internet hi-jackers (even cracker-packers!) . . .

IT IS!!

Build a digital moat around your personal information and then consider the following 10 simple ways you can protect yourself.



1. Give your Password a quick Pump up!

Eight characters or more are the best (the more, the merrier). Include numbers and special characters, and avoid using names or words associated with you. Never use the same password for multiple accounts, and be sure to change your passwords regularly. Every three months is considered the best

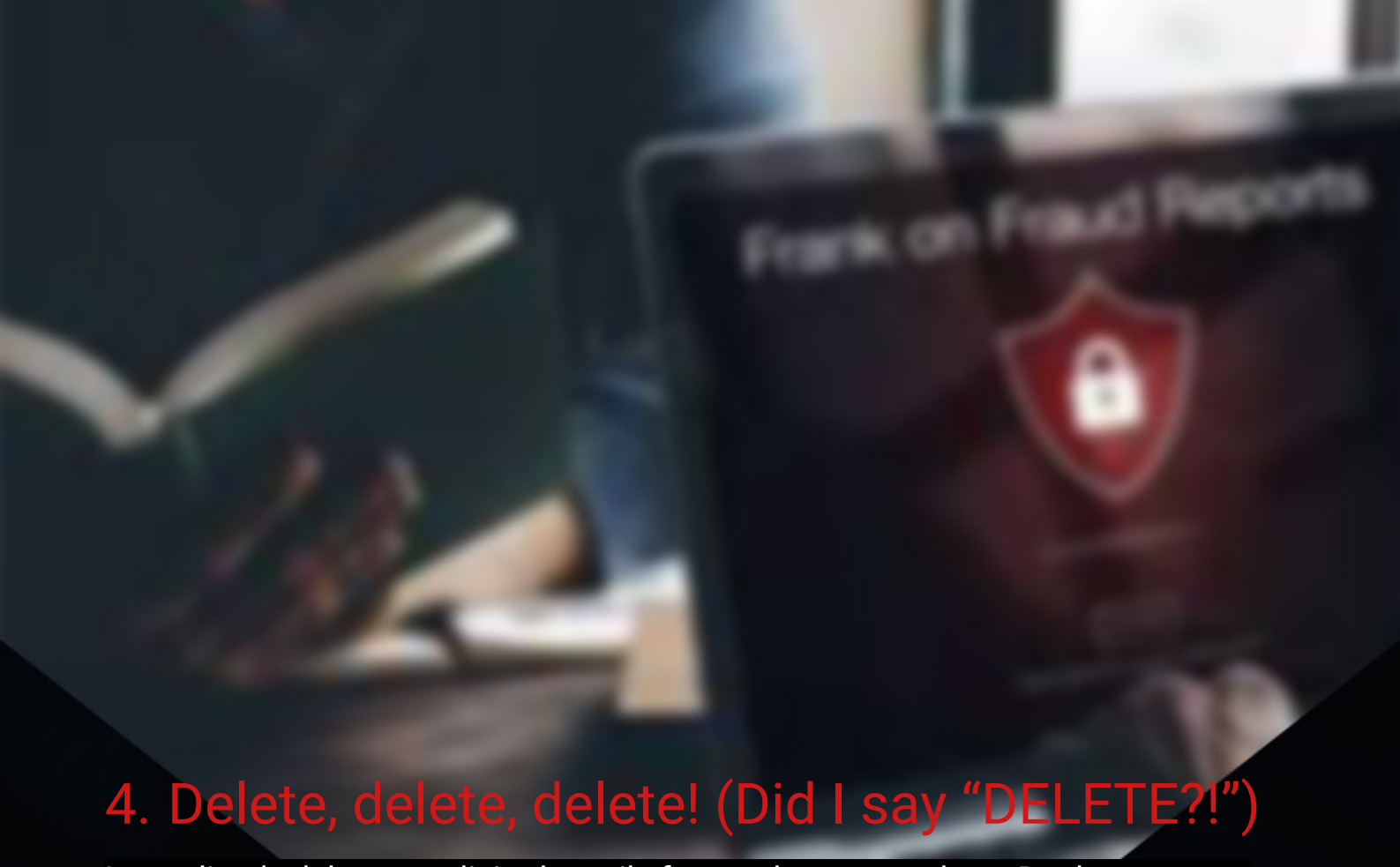
2. Check out the Sender!

Legitimate banks, financial institutions, credit agencies, as well as any legitimate business will not ask for passwords, account numbers or any personal financial information by email. If you decide you need to respond, then exit the email and log on separately to the official website of the sender. Never click on a link inside the email! Hackers "Clone" official websites to fool unsuspecting people.

3. Check out those links!

Hover your mouse over the link to see the true destination. For most internet browsers, the link can be seen in the bottom left corner of your device. If it's different than what's shown in the email, watch out! It could be a scam.

Please note: links leading to .exe files are known to spread malicious software.



4. Delete, delete, delete! (Did I say “DELETE?!”)

Immediately delete unsolicited emails from unknown senders. Don’t even open them! Sometime opening them, activates a download, wanted or unwanted, and could really create a bad-computer day and bad-hair-day for you! Never forward a suspicious email to family, friends, or co-workers – even as a warning!

5. Don’t fall victim to Threats!

The old saying, “Sticks and stones may break my bones, but WORDS (Threats!) will never hurt me!” Cybercriminals often use threats, “Your account will be closed if you don’t respond to this email!” or just outright lies, “We’re gonna come and throw your whole family in prison and fine you the equivalent of a small nations’ gross national product if you don’t respond! Or simply, “Your security has been compromised” in an effort to get you to take action. These words have the ability to scare the pudding out of you, so be extra suspicious of emails requiring immediate action.

6. Look for the Padlock!

When shopping or banking online, look for a padlock symbol in the web browser. Don’t give out one digital letter of any private or personal information unless you see this in the upper left corner of your favorite web browser. This, along with web addresses that begin with https:// indicate extra security measures. The “S” stands for secure. And if you don’t see it, the “S” can also stand for “STUPID!”

Be pro-active, not re-active! Don't wait till you have been hacked and are living in internet jail before you get serious about it!

7. Use Safe Payment options

Most credit card issuers allow you to seek a credit if your product isn't delivered or differs from what you ordered. Insuring your purchases are safe will save you having to take some headache medication after your shopping experiences and prevent you from explaining to your spouse why the "Blinker Fluid" you ordered online for $179.95 never showed up!

8. Be Savvy with Security Software

Protect your devices with anti-virus, anti-spam and other "anti-enter your own internet word here" software. Regularly install updates to programs and applications as they often include improved security settings and measures.

9. Take the Wimp out of your WI-FI security!

Protect your Wi-Fi with a strong password that only your family knows. Don't let your dog or cat in on it – they'll give it up every time they're interrogated! Also, don't use unsecured networks when you're out and about (common sense, right?!). Free Wi-Fi at your favorite caffeinated drink station may not be as free as you would like.

10. Keep Private Things Private!

Privacy settings on all your social media accounts need to be checked and updated from time to time. Mr. Zuckerberg (and others) tends to make occasional changes to privacy policies causing you to wonder how your brothers' tree and lawn service managers' young sons' picture post of his latest creative poo-poo ended up in your Facebook news feed! Make sure only the people you want to share your information with can see it.

This short report was inspired by article in Modern Woodmen Magazine, by Leah Eigenbrod, but curation and color-commentary has been provided by Walter Nigh. :)

For more information and help regarding your online security, check out Walter's online training program, "First Steps Online." His comprehensive training includes more ways on how to secure your online experiences. **Check it out HERE!**

THANK YOU

Walter Nigh

Online Marketer and author of several training programs and online training publications.

More online training and coaching at **WORK-WITH-WALT.com**

Connect on Facebook at: **Online Income Strategies**