



21 West 38<sup>th</sup> Street, 14<sup>th</sup> Floor, New York, NY 10006 Phone: (888) 336-6884 ext. 1 Fax: (212) 363-9526 [www.horsemouth.com](http://www.horsemouth.com)

## A Cybersecurity Survival Guide for the “You’ve-Been-Hacked” Era *Stopping Hackers, Identity Theft, and Malware Scams Is Easier Than You Think—The New Cybersecurity Rules*

NEW YORK, NY, October 2016 – Anyone who has ever searched on Google and, 30 minutes later, found themselves endlessly clicking links knows the power the Internet can exert over our time and attention.

It’s no surprise, then, that cyber criminals try to exploit our inattentive email and website clicking.

In just the next 24 hours:

- Scammers will target the public with 94 billion emails
- Hackers will seize and hold 88,000 computers for ransom
- Identity thieves will impersonate 35,000 people

Everyone is besieged by a nonstop cyber-crime wave that victimizes millions of people and businesses each year. And trouble usually starts with a click.

Can anyone really be safe and secure online? Yes, there is a way to quickly shut down hackers, thieves, and identity scammers and enjoy good online security, say Sean M. Bailey and Devin Kropp, the authors of a new book, *Hack-Proof Your Life Now! The New Cybersecurity Rules* (Horsemouth, LLC., 2016, ISBN 978-0-9977290-0-9, Paperback \$19.95, [hackproofyourlifenow.com](http://hackproofyourlifenow.com)).

Bailey and Kropp are the creators of an educational workshop called “One Hour to Savvy Cybersecurity.” They contend that anyone can dramatically boost their online security by taking a handful of inexpensive and easy-to-accomplish actions.

Their book begins by asking the reader to measure his or her online security with a 10-question cybersecurity quiz. Nearly everyone scores poorly. But that changes quickly as the authors introduce the New Cybersecurity Rules, a set of 15 principles organized around three mindsets that must be cultivated in order to achieve higher security:

1. **Secrecy.** Email addresses, passwords, credit files, Social Security numbers, and other personal information need greater levels of protection. Governments and private companies have done a miserable job guarding personal data, the authors point out. Only individual actions can limit exposure to hackers’ data breaches. The authors offer eight secrecy-boosting rules, including this one: Stop using a personal email address for online banking and credit accounts. It’s too easily stolen. Instead, create a financial-only email account to use exclusively for finances. That limits exposure to just a few secure places on the Internet where the financial-only email resides, making it harder for hackers to scoop up and exploit.

2. **Omniscience.** Just like the financial services industry, consumers must use technology to become “financially all-knowing” and monitor—in real time— personal banking and credit matters, Bailey and Kropp say. By placing one's self at the center of online security (a key theme of the book), everyone can rest assured that identity thieves aren't quietly stealing their money or ruining their credit. One recommended omniscience rule: Set up notifications on banking and credit cards to instantly become aware whenever cash leaves any accounts or when credit is charged. It's a way to instantly spot fraud or identity theft, a solid protection to have at no extra cost.
3. **Mindfulness.** Enacting the New Cybersecurity Rules instills a stronger security mindset, the authors tell us. But how can it be maintained? Safety degrades without permanent changes to computer behaviors and security awareness. For instance, part of staying hack-proofed is routinely updating software to close dangerous security holes or backing up data to protect against cyber blackmail. Just like cars, the authors remind us that critical maintenance must be applied to computers, tablets, and smartphones to keep cyber miscreants away.

But the hackers never sleep, sending an estimated 34 trillion emails per year. Even the best protected inbox will still receive a few dangerous emails. What to do? The authors suggest their 10-Second EMAIL Rule, an easy to remember mnemonic for staying mindful of avoiding malicious links. EMAIL stands for “Examine Message and Inspect Links” and shows how to spot and unmask dangerous blackmail spam and identity theft malware. It's a Zen-like practice that can benefit everyone every time they check their email.

While many cybersecurity titles focus on criminal networks, cyberwarfare, or lengthy lists of online security threats that people and businesses face, *Hack-Proof Your Life Now!* takes a more practical approach. The completion of each action-step associated with the New Cybersecurity Rules raises the reader's cybersecurity score. They realize they're not helpless. The sum total of adding more secrecy, enacting financial omniscience, and adopting mindful computing practices boosts online security in real terms. And in this era of “You've been hacked,” that's saying something.

###

#### **About the Authors:**

Since 1999, Sean M. Bailey has been the editor in chief of Horsemouth, a New York-based company that creates educational programs on retirement planning, Social Security, Medicare, college planning, and cybersecurity. Devin Kropp is an associate editor at Horsemouth specializing in cybersecurity. Bailey and Kropp created the Savvy Cybersecurity training program in 2014. It has been presented hundreds of times in the U.S. and Canada.

#### **About the Book:**

Boost your online security quickly with *Hack-Proof Your Life Now!* (Horsemouth, LLC., 2016, ISBN 978-0-9977290-0-9, Paperback \$19.95, [hackproofyourlifenow.com](http://hackproofyourlifenow.com)).

#### **Review Copies and Media Interviews:**

Please contact [hackproof@horsemouth.com](mailto:hackproof@horsemouth.com) or (212) 217-1130 for interviews or review copies. When requesting a review copy, please provide your street address.

# Data Sheet

**Title:** Hack-Proof Your Life Now!

**Subtitle:** The New Cybersecurity Rules: Protect your email, computers, and bank accounts from hacks, malware, and identity theft

**Description:**

Everyone is vulnerable to a cyber attack. Regardless of your age and station in life, one simple click of the mouse can open a Pandora's box few of us could have imagined even five years ago.

How we handle our online security is critical to protecting our personal and professional lives. But guidance for staying safe in the growing, interconnected world has been fragmented and confusing—until now.

*Hack-Proof Your Life Now!* demystifies the topic and introduces you to the New Cybersecurity Rules—clear, sensible, and do-able actions that will quickly improve your security.

Authors Sean M. Bailey and Devin Kropp will show you how to measure your Cybersecurity Score and then teach you to improve your safety by acting in three areas: adding more Secrecy to your online life (such as a banking-only email address that hackers won't likely discover), becoming Omniscient over your financial affairs (so you can block identity theft and instantly spot fraud), and adopting principles of Mindfulness to stay safe every day (such as using their 10-Second EMAIL rule to spot dangerous blackmail spam).

Each chapter features a Hack Report story that demonstrates a key security problem many of us face, a New Cybersecurity Rule that reduces or closes that exposure, and a specific Action Step to apply as you build up your defenses and improve your cybersecurity score. An Action Guide in the back provides extra details and helpful resources.

In just a few hours, you can learn to hack-proof your life and fight back against hackers, thieves, and spammers.

**Price:** \$19.95 Paperback, 227 pages

**ISBN:** 978-0-9977290-0-9

**Publication Date:** October 25 2016

**Contact Information:**

Horsemouth, LLC.  
21 West 38th Street, 14th Floor  
New York, NY 10018  
(212) 217-1130  
hackproof@horsemouth.com

## Author Biographies

**Sean M. Bailey** is the co-creator of the Savvy Cybersecurity training program, an interactive workshop to teach people to boost their online security. He is the co-author, along with Devin Kropp, of *Hack-Proof Your Life Now! The New Cybersecurity Rules: Protect your email, computers, and bank accounts from hacks, malware, and identity theft*.

Bailey is the founding editor in chief of Horsesmouth ([www.horsesmouth.com](http://www.horsesmouth.com)), a Manhattan-based company that creates educational programs on retirement planning, Social Security, Medicare, college planning, and cybersecurity for industry professionals from top firms including Ameriprise, LPL, Merrill Lynch, Morgan Stanley, Northwestern, Raymond James, and UBS.

He was an early promoter of the Internet in the 1990s and led a national conference series teaching nonprofits about technology, building websites, and raising money online.

Bailey pioneered computer-assisted reporting in the late 1980s, along with his colleagues at the *News & Observer* of Raleigh, using public-record data to probe government programs. He was honored by the North Carolina Press Association for his investigative reporting, covering local politics and white-collar crime.

Bailey's interest in fraud started as a college journalist at Appalachian State University when his reporting about a vote-buying scheme in Western North Carolina upset local authorities and triggered a grand jury investigation. Bailey was a Peace Corps Volunteer in Belize. He lives with his wife and daughter in Maplewood, New Jersey.

**Devin Kropp** is the co-creator of the Savvy Cybersecurity training program, an interactive workshop to teach people to boost their online security. She is the co-author, along with Sean M. Bailey, of *Hack-Proof Your Life Now! The New Cybersecurity Rules: Protect your email, computers, and bank accounts from hacks, malware, and identity theft*.

Kropp is an associate editor at Horsesmouth and the lead researcher for the monthly Savvy Cybersecurity newsletter. She first experienced the shock associated with identity theft as an 11-year-old in 2002. Just before Christmas, hackers stole her father's debit card information and sold it to a thief in Spain, who drained several thousand dollars from the account. Kropp is a graduate of Binghamton University, State University of New York, where she studied English and journalism, and played wing and scrum-half for the Women's Rugby Club. She lives in Manhattan.

### Contact Information:

Horsesmouth, LLC.  
21 West 38th Street, 14th Floor  
New York, NY 10018  
(212) 217-1130  
[hackproof@horsesmouth.com](mailto:hackproof@horsesmouth.com)

## **Interview with Sean M. Bailey, Co-Author of *Hack-Proof Your Life Now!***

### **Why did you write *Hack-Proof Your Life Now!*?**

Back in 2013, we'd been following the growing concerns about identity theft for quite a few years. We work with financial planners and it's a topic many of their clients are deeply concerned about. Once the Target breach hit late that year, we began to realize a few things: Everyone's personal identifiable information is at risk. The companies and institutions we've shared that information with have done a terrible job of protecting it. The online security advice being offered to the general public seemed fragmented, overwhelming, wrong, or incomprehensible. Yet, we could see that there were clear, sensible steps anyone could take to easily improve their security. Even today, you'll read an article in a major national newspaper or website about a new threat—say, for instance, the growing threat of ransomware against people or their employers. The article will be intriguing, well-written, and researched, yet it will often offer *no* discussion about the steps anyone can take to inoculate themselves or their company against falling victim to the blackmail threats of ransomware. The public gets all the scare and not a single solution. In our book, we certainly take the time to tell our readers stories about the new threats and types of victims who've succumbed. But then we give them do-able solutions. We tell you exactly what you need to do to ensure that you don't suffer the same way. We didn't see anyone really offering a personal system of consolidated and do-able actions that measure and boost your cybersecurity.

### **What experience do you have in the field of cybersecurity?**

In 2014 we created an interactive workshop called “One Hour to Savvy Cybersecurity” and made it available to financial professionals to deliver in their communities in the United States and Canada. It has since been delivered hundreds of times to extremely good reviews.

During that time, the problems with hacking and cybersecurity continued to grow, as we've all witnessed. We decided we needed more ways to get our key message across to the public and that included writing a book that could be quickly read and acted upon.

### **The first word in your book is “click.” It's the set up for your introduction. But you come back to the click in the final section of the book, too. Why is the click so important to cybersecurity?**

Clicking is the first thing everyone learns when they first encounter a computer and the Internet. The click and its partner, the link, are the most elemental aspects of how the Internet, email, computers, and the World Wide Web work. The link, as we say, courts the click. That's where the trouble begins.

The TV channel changer was our first introduction to the click. Push a button and the screen changes. It's the same with computers: click a link and the screen changes. The TV version is innocuous. The computer version is potentially dangerous. With one errant click, you can suddenly turn your computer over to the hackers.

### **What makes your book different from others about cybersecurity and identity theft?**

Many books on cybersecurity fall under one of two types: They're either about criminal networks, terrorism, the potential for global cyber warfare, or they're very detailed, comprehensive listings of cybersecurity threats faced by individuals and businesses with technical suggestions about what to do to blunt the threats. The first type of book is provocative and entertaining and the second type of book is overwhelming and dispiriting. In either case, people are left feeling paranoid or helpless. We wanted to write an engaging book that gets people to act to improve their cybersecurity quickly and easily. We feel we've done that by identifying a small, core group of actions people need to take in three areas, which we've labeled Secrecy, Omniscience, and Mindfulness. When you put these in place, you're vastly more secure.

**Secrecy, I understand. But Omniscience and Mindfulness don't sound like concepts we'd normally associate with cybersecurity. Can you tell us a little more about all three?**

We view *Hack-Proof Your Life Now!* as a self-help title. It gives you an easy framework through which to view your online security and improve it by taking clear, do-able action steps in each of three main areas.

The first is Secrecy. We all need to add much more stealth to our digital lives. We know from the massive data breaches, for instance, that many people set up their email and passwords in very casual, haphazard, and insecure ways that make their email accounts, and often their banking and other financial accounts, extremely vulnerable to hacking and identity theft. There are do-able, fast steps one can take to increase your secrecy and improve security. For instance, people tend to have one or two main email addresses that they use for nearly everything—work, personal matters, and their financial affairs. You don't want the email address and password you use for Pinterest or ESPN to be the same ones you use for your online banking, credit cards, and other financial sites. That's an invitation to disaster. We recommend creating an exclusive, secret, financial-only email address and password to use just for the handful of accounts that involve your finances. By doing that, you've reduced your "digital footprint" to only those highly secure institutions and your email provider. If hackers steal or sell your credentials stolen from some other site, it won't give them any insight or potential to break in or impersonate you at banking or other financial websites. That's one example of how to increase your secrecy and boost your security. We offer eight secrecy-boosting actions in that section of the book and each one only takes a few minutes to implement.

The second area is Omniscience and what we mean here is that you should become "financially all-knowing," or omniscient, over your financial affairs. This means that you should use technology to easily monitor the flow of money out of your bank accounts and the charges made against your credit and debit cards. This is very easy to do. Your bank and credit card companies provide the notification systems that allow you set up an early-warning system against identity theft and fraud. If your card number has been stolen and sold into the black market, as soon as a hacker attempts to use it, you'll see the first charge come through your notification system, you'll know something is wrong, and you'll be able to take action and shut down the hacker. This costs nothing to set up. The key thing to keep in mind here is that the banks and credit card companies know up to the minute what's happening in your accounts. There's no reason you shouldn't also have that same level of omniscience or financial all-knowingness. You're best equipped to spot fraud and keep yourself safe—not anyone else. It's not a job that can or should be outsourced. It's too important. We offer four actions in the Omniscience

section of the book that together create a system that puts you at the nexus of your personal finances and your credit. When you do that, you know what's happening in your financial life and you can be more confident that you're safe and secure from hackers.

The third area is Mindfulness. Online security is a very fluid and changeable. It's not unlike an old car. Once you get it tuned up and humming, it runs along nicely but slowly degrades over time. The same with your cybersecurity. Once you've boosted your security, you won't stay permanently secure *unless* you adopt certain regular practices that will update and renew your safety. This is where mindfulness comes in and it involves two things:

The first is about changing some of your behaviors around computer and online security—we're often operating under wrong assumptions and mistaken beliefs that make us much less safe. For instance, most computer technicians will tell you that when they're called to fix a computer that has succumbed to some sort of hack or virus, the problem often stems from people using out-of-date software that typically has dozens, if not hundreds, of known security holes that were closed in the past through software updates people never bothered to complete. Nearly every computer security expert will tell you that updating your software is one of the most important things you can do to stay safe from hackers. It's simple digital hygiene, really. Yet the average person tends to ignore updates, often for reasons that actually aren't true—such as the idea that updating software will change their user interface or that an update will cause them to lose information they're currently working on. Neither is true. This is one aspect of Mindfulness. We need to accept the critical importance of updating software, take a breath, and simply do it. It's nearly always painless and takes just a couple of minutes. It's not unlike filling up your car and checking the oil.

The second aspect of Mindfulness involves learning to be vigilant and guarding against falling for the common, growing deceptions related to malware and ransomware. In this case, we teach our readers how to implement our 10-Second EMAIL Rule. We've designed this simple to remember and easy to implement mnemonic to help people unmask the malicious email links that do the most harm and damage when people unknowingly click on them. In our rule, EMAIL stands for "Examine Message and Inspect Links". We teach people how to systematically look at any email or link and quickly determine its malicious intent without being scammed and suddenly losing control of their computer and their security.

All the actions we recommend people take in *Hack-Proof Your Life Now!*—about 15—build a personal security system that costs little to nothing to implement, puts you in complete control of your security, and gives you the insights and confidence to remain safe and secure every day.

**Many people seem overwhelmed by cybersecurity. How does *Hack-Proof Your Life Now!* combat that?**

Feeling overwhelmed and not taking action is a major reason people have such poor cybersecurity and why hackers are so successful. Internet security experts can come up with a nearly endless list of potential threats we all face. That's one of the reasons we wanted to write *Hack-Proof Your Life Now!*

We start by having people measure their current level of cybersecurity. We give them a specific Cybersecurity Score after they answer 10 yes or no questions at the beginning of the book. Most people score very low. But then we show them the easy steps to quickly achieve higher security.

What we've done is identify key, major security threats everyone faces and the most effective preventative measures people can take to block those threats and raise their Cybersecurity Scores. That's really a little more than a dozen actions that, when completed, will dramatically improve your security. As people go through *Hack-Proof Your Life Now!*, they'll see each short chapter gives them a concrete action step that usually can be completed in just minutes. And if the action involves an aspect of computers and the Internet that they simply don't understand, we reference our Action Guide in the back of the book which gives deeper, step-by-step instructions. But nearly every action we recommend can be easily accomplished, often within just a few minutes.

**For many people, their biggest fear about cybersecurity seems to be identity theft. What does *Hack-Proof Your Life Now!* recommend for people worried about this that is new?**

Most people still don't realize the importance of two-step verification for their email and financial accounts. Very few people do this even though it is now widely available and easy to accomplish. It's a great feature because you'll be instantly notified if any hacker starts hammering at your accounts. Should a hacker get as far as knowing and using a valid username to access your email or any financial account, they'll be stopped and you'll be notified with the alert to complete the second part of the login process. Since you didn't initiate the first part and the hacker can't receive the second part, you'll know a failed attempt to hack your account has transpired and you can investigate. But as long as you have the second part of the two-step login, you'll know you're safe. Hardly anyone is putting two-step verification on their email and financial accounts.

**Regarding identity theft: can't people just sign up for credit monitoring and be secure from theft or some other security intrusion?**

We're often asked by people if they should sign up for credit monitoring services offered by LifeLock or the big three credit agencies—Experian, Equifax, and TransUnion. The simple answer is no. We don't recommend these monitoring services because they epitomize closing the barn door after the horse has fled. If a credit monitoring service contacts you about some activity in your credit file that you did not initiate, then you already have an identity theft problem. The credit monitoring service is just informing you of that problem. That's not hack-proofing your life.

There's a much better way to protect yourself against identity theft and the companies offering protection services don't typically tell you this. When you put a Credit Freeze, known technically as a Security Freeze, on your credit files at the three credit reporting agencies, your files are closed and completely secure. There's no way an identity thief can add credit to your file by impersonating you. You're safe and you have total control over your file when it is frozen—only you can lift the freeze. This costs little or nothing to implement and is basically fool-proof. The Credit Monitoring services typically cost about \$150-\$300 a year and yet you're still vulnerable to identity theft. We don't recommend people spend their money on a service that doesn't give them maximum protection,

especially when they can be much safer by taking control of their credit files and putting them on a Security Freeze.

This speaks to one of our key messages: You should be in complete control and all-knowing over your financial affairs. Knowing your credit file is off-limits to identity scammers because you've put a freeze on the file is a good example of Omniscience over one's cybersecurity. Doing the same for your minor children is another example.

### **What is the biggest cybersecurity threat faced by the most people?**

We think clicking on a malicious link in an unsolicited email poses one of the greatest threats people face. That simple action can open a Pandora's Box of trouble. Sometimes you'll know it was a problem instantly—the hackers will lock up your computer with powerful encryption software and demand ransom to give it back. Other times, you'll have quietly opened the door to your computer—and your organization's computer network, if you're on your work computer—and the hackers may set up shop, secretly recording keystrokes, passwords, emails, files, etc. That's why we think it's so important for people—individuals at home and employees at work—to know how to mindfully view any suspicious email. That's why the 10-Second EMAIL Rule is so important. Everyone needs to stay calm and examine any email that seems the least bit strange or out of character.

### **Are there any people who need cybersecurity more than others?**

For the most part, everyone—every individual and every employee with access to the Internet—needs to have solid, high cybersecurity scores in order to be safe personally and professionally. This is a major challenge, especially for corporations and institutions. Think about this: before the age of personal computing and the Internet, an organization's security was mostly conceived of in terms of physical security. The most sensitive or valuable information would be under some sort of “lock and key” protection. Whatever was being guarded could only be accessed physically. Those locations would be closely monitored. You'd need a special pass or clearance to get in. You'd need to sign-in or be searched before and/or after having contact with whatever was being guarded. All of this would be segregated so that in some organizations only select people would have access to such sensitive information. A company might have 100,000 employees but maybe less than a dozen had access to the “crown jewels” that were under close watch and lock and key.

Now, in the age of computing and the Internet, that same company with 100,000 workers now has 100,000 points of vulnerability—not a dozen. Any one of their employees with access to a computer and the Internet could inadvertently click a link that opens the company's computer network to hackers. We've seen this sort of thing in many places in recent years. It takes one employee with one click on one malicious link and in come the hackers. What happens next is anyone's guess. The upshot is that everyone in any organization needs to have a solid understanding of cybersecurity and their responsibility to act safely.

### **How does *Hack-Proof Your Life Now!* actually get people to act and make changes to their cybersecurity?**

Each short chapter deals with one specific type of security threat and one set of actions we recommend people take to close that threat and boost their Cybersecurity Score.

There are about 15 actions for people to take as they move through the book's three areas. At the end, we organize them by type—some require actions you can take with your computer, others involve actions you must take with any financial services company you do business with, and other actions involve things you must begin adopting as part of your daily, Internet security practices. We've organized those into an easy to use checklist at the end of the main section of the book.

Finally, in the back we've included an in-depth Action Guide. If there's any recommendation we make in the main part of the book that the reader doesn't understand, they can turn to the Action Guide for additional, in-depth, and step-by-step guidance on implementing a specific action. Overall, most people will be able to complete the action steps without a need to consult the Guide in the back.

### **What's the biggest take-away from *Hack-Proof Your Life Now!*?**

We don't live in the innocent "You've-Got-Mail" era anymore. Online security is critical for everyone from the highest ranking government or corporate official right down to the youngest, newest user of the Internet and email. We're all equally vulnerable to the growing range of hacker threats. It takes just one wrong click to let the bad guys in. Nearly every major hack we know of started with the seemingly innocent action of one person. We all have to be in charge of our security; we have to be at the center of our personal internet security system. This cannot be completely outsourced to some other person or company. Just like nearly everyone has learned to drive and respect the rules of the road, we each need to accept personal responsibility to hack-proof our lives by implementing a small group of easy to accomplish actions. It's totally within our abilities to dramatically beef up our security.

### **What's one thing people will learn that they've not seen or heard elsewhere?**

Our 10-Second EMAIL Rule – "Examine Message and Inspect Links"—is not something readers will have seen elsewhere. Learning this rule and making it part of your everyday thinking will vastly reduce your vulnerability to hackers when it comes to ransomware or other malware attacks. The blackmail bill for paying hackers to release your files can run from around \$500; well up into the tens of thousands for companies. So learning the EMAIL Rule can be beneficial to anyone's wallet and their sanity.

### **Don't things change so fast that a book about cybersecurity will be outdated in 12 months?**

Actually, no. That's a bit of myth. The threats change or evolve, but the core actions needed to have good cybersecurity don't. It's true that 12 months from now there may be some new types of cyber threats. The core cybersecurity practices that we recommend to hack-proof your life were powerful and relevant five years ago and we expect they'll still be powerful and relevant five years from now. We expect that there will be some new, innovative ways to boost your security in the future, but the core principles at the heart of *Hack-Proof Your Life Now!* will still be relevant five years from now, too.

### **What does the future hold for cybersecurity?**

Interview with Sean M. Bailey, Co-Author of *Hack-Proof Your Life Now!*  
21 West 38th Street, 14th Floor, New York, NY 10018; (212) 217-1130; hackproof@horsesmouth.com

We won't be surprised to see governments and corporations start to measure people's cybersecurity knowledge as an important part of the hiring process. You may recall the old World War II security adage: "Loose lips sink ships." That was an acknowledgment that everyone in society bore some responsibility for national security. Now that we're in the age of personal computing and the Internet, we might update that adage to say: "Bad clicks sink ships." The damage done to organizations and corporations as a result of poor security practices has had devastating effects. We've seen CEOs and other C-suite people fall from power following a data breach or cyber attack. Expect to see a much wider and deeper emphasis on cybersecurity skills within organizations. It can no longer simply be an issue only for the IT guys. Everyone needs to boost their online security.