SENIOR CYBER

Best Security Practices for Your Golden Years

SCOTT N. SCHOBER
with Craig W. Schober

Senior Cyber: Best Security Practices for Your Golden Years

Published by ScottSchober.com Publishing
Metuchen, New Jersey

Hardcover ISBN: 978-0-9969022-9-8
Paperback ISBN: 978-1-7363158-0-4
eISBN: 978-1-7363158-1-1

Cover and Interior Design by GKS Creative
Copyediting and Proofreading by Kimberly A. Bookless
Illustrations by Jake Thomas of Jake Thomas Creative
Project Management by The Cadence Group

This book may be purchased for educational, business, or sales promotional use. For information, please email info@scottschober.com, call 732-548-3737, or visit www.ScottSchober.com.

Appendix: Senior Scams and What to Look For

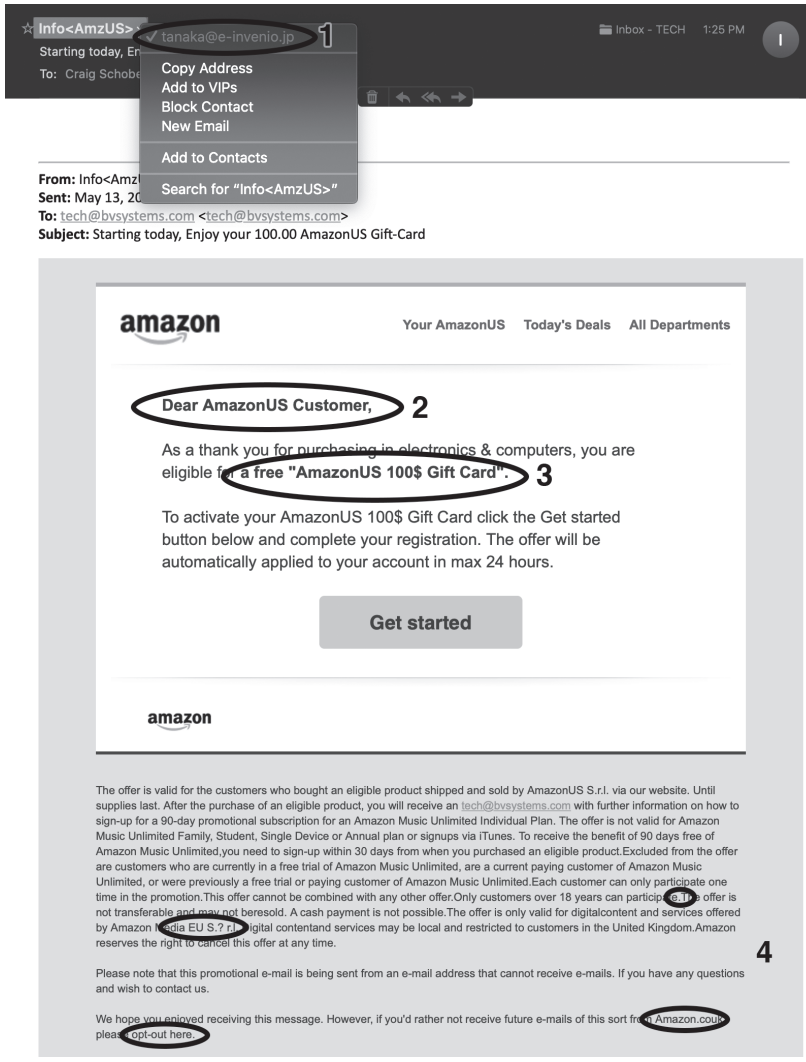
This information will help you identify email scams quickly. Remember that the goals of the scammers can vary. Some scammers want to dupe you into sending them money. However, others simply want you to click on the obvious link in the email itself or open an attachment so harmful malware can be immediately downloaded to your computer.

Depending on the type of malware or destination of the URL link, a number of things can happen to your private data, including your passwords and account numbers:

- it can be taken and used in identity theft;
- your credit card information can be stolen and used for fraudulent purchases;
- your contacts can be harvested and sold to other scammers;
- as in the case of John Podesta, your private emails and other communications can be stolen and used to harm you or others (possible extortion); or
- your entire computer contents can be frozen until you pay the scammer/hacker a ransom to unlock it.

Note that these are just a few reasons to become aware of email scams and have a robust antivirus program like Avast that scans your computer in the background for the latest threats. And make sure it is constantly running the latest updated version.

Below are examples of some common email scams you might encounter.



A SCAMMER PRETENDING TO BE AMAZON:

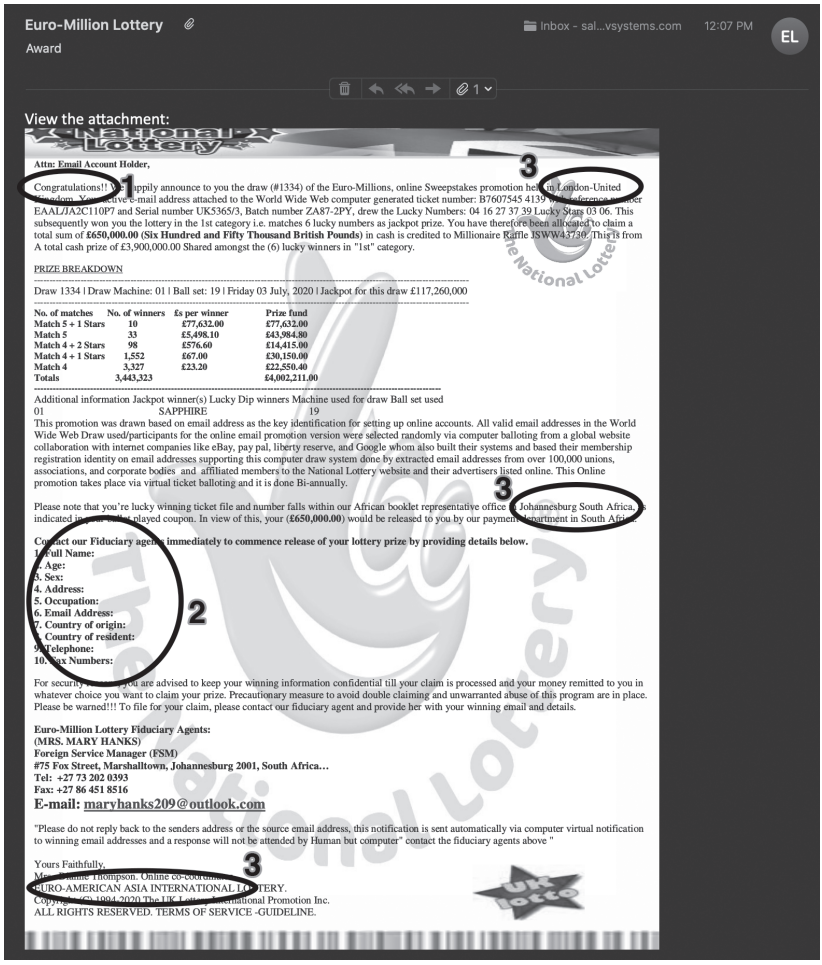
1. The "From" category of email scams can be deceiving. For example, it appears

that this email is from Amazon, but you can easily click on the sender's email name to see the actual sender's email address, which *should* be from Amazon.com. In this case, though, it looks like the email came from some scammer with an "e-invenio.jp" server domain. The ".jp" indicates the server is in Japan, even though the email references Amazon in both the United States and Great Britain.

2. If you have an Amazon account, you can be sure the company knows your full name and other important information. However, since scammers rarely know much (if anything) about you, they might address you as "AmazonUS Customer" because they don't know your real name.
3. Notice the syntax, spacing, bold type, and use of quotes in: **a free "AmazonUS 100$ Gift Card".** This is sloppy and oddly phrased for a trillion-dollar company like Amazon with a professional marketing

department that sends out millions emails every single day; the real Amazon does not make these kinds of mistakes.

4. In the fine print at the bottom, notice all the tiny punctuation errors, lack of proper spacing, and missing links. The terms appear to match legitimate Amazon emails, but that's because the scammers simply copied and pasted bits from real Amazon emails. However, they neglected to assemble the bits back into a proper fashion, so it looks strange.



Euro-Million Lottery
Award

Inbox - sal...vsystems.com 12:07 PM EL

View the attachment:

Attn: Email Account Holder,

Congratulations!! We happily announce to you the draw (#1334) of the Euro-Millions, online Sweepstakes promotion held in London-United Kingdom. Your active e-mail address attached to the World Wide Web computer generated ticket number: B7607545 4139 with reference number EAAL/JA2C110P7 and Serial number UK5365/3, Batch number ZA87-2PY, drew the Lucky Numbers: 04 16 27 37 39 Lucky Stars 03 06. This subsequently won you the lottery in the 1st category i.e. matches 6 lucky numbers as jackpot prize. You have therefore been allocated to claim a total sum of **£650,000.00 (Six Hundred and Fifty Thousand British Pounds)** in cash is credited to Millionaire Raffle JSWW43736. This is from A total cash prize of £3,900,000.00 Shared amongst the (6) lucky winners in "1st" category.

PRIZE BREAKDOWN

Draw 1334 | Draw Machine: 01 | Ball set: 19 | Friday 03 July, 2020 | Jackpot for this draw £117,260,000

No. of matches	No. of winners	£s per winner	Prize fund
Match 5 + 1 Stars	10	£77,632.00	£77,632.00
Match 5	33	£5,498.10	£43,984.80
Match 4 + 2 Stars	98	£576.60	£14,415.00
Match 4 + 1 Stars	1,552	£67.00	£30,150.00
Match 4	3,327	£23.20	£22,550.40
Totals	3,443,323		£4,002,211.00

Additional information Jackpot winner(s) Lucky Dip winners Machine used for draw Ball set used
01 SAPPHIRE 19

This promotion was drawn based on email address as the key identification for setting up online accounts. All valid email addresses in the World Wide Web Draw used/participants for the online email promotion version were selected randomly via computer balloting from a global website collaboration with internet companies like eBay, pay pal, liberty reserve, and Google whom also built their systems and based their membership registration identity on email addresses supporting this computer draw system done by extracted email addresses from over 100,000 unions, associations, and corporate bodies and affiliated members to the National Lottery website and their advertisers listed online. This Online promotion takes place via virtual ticket balloting and it is done Bi-annually.

Please note that you're lucky winning ticket file and number falls within our African booklet representative office in Johannesburg South Africa, as indicated in your e-mail played coupon. In view of this, your (**£650,000.00**) would be released to you by our payment department in South Africa.

Contact our Fiduciary agent immediately to commence release of your lottery prize by providing details below.
1. Full Name:
2. Age:
3. Sex:
4. Address:
5. Occupation:
6. Email Address:
7. Country of origin:
8. Country of resident:
9. Telephone:
10. Fax Numbers:

For security reasons, you are advised to keep your winning information confidential till your claim is processed and your money remitted to you in whatever choice you want to claim your prize. Precautionary measure to avoid double claiming and unwarranted abuse of this program are in place. Please be warned!!! To file for your claim, please contact our fiduciary agent and provide her with your winning email and details.

Euro-Million Lottery Fiduciary Agents:
(MRS. MARY HANKS)
Foreign Service Manager (FSM)
#75 Fox Street, Marshalltown, Johannesburg 2001, South Africa…
Tel: +27 73 202 0393
Fax: +27 86 451 8516
E-mail: maryhanks209@outlook.com

"Please do not reply back to the senders address or the source email address, this notification is sent automatically via computer virtual notification to winning email addresses and a response will not be attended by Human but computer" contact the fiduciary agents above "

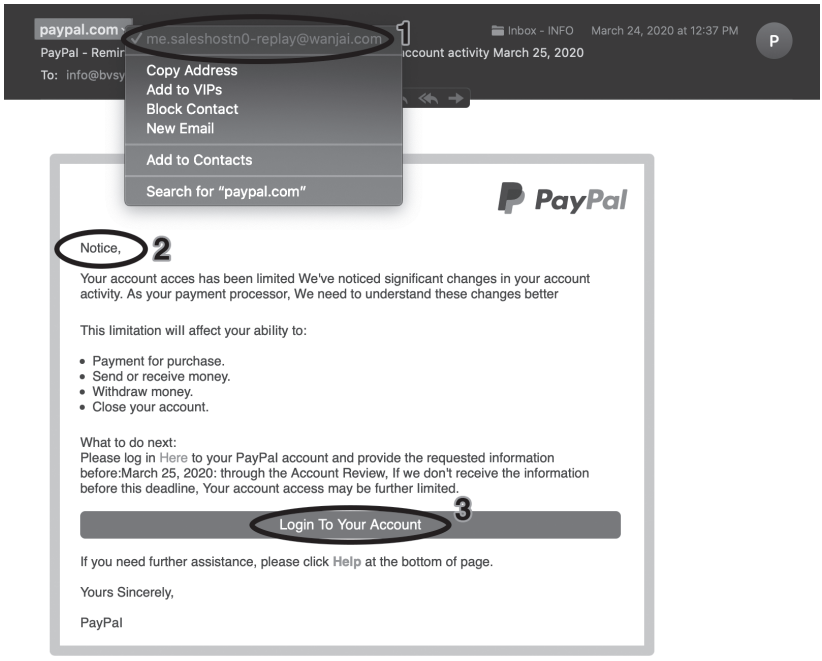
Yours Faithfully,
Mr. Jamie Thompson. Online co-coordinator
EURO-AMERICAN ASIA INTERNATIONAL LOTTERY.
Copyright © 1984-2020 The UK Lotto International Promotion Inc.
ALL RIGHTS RESERVED. TERMS OF SERVICE -GUIDELINE.

A SCAMMER PRETENDING TO BE A LOTTERY COMMISSION:

1. If you receive a congratulatory email for winning any kind of contest you did not enter, it is a scam—especially if it

appears to be from the "Euro Lottery," which doesn't even exist.

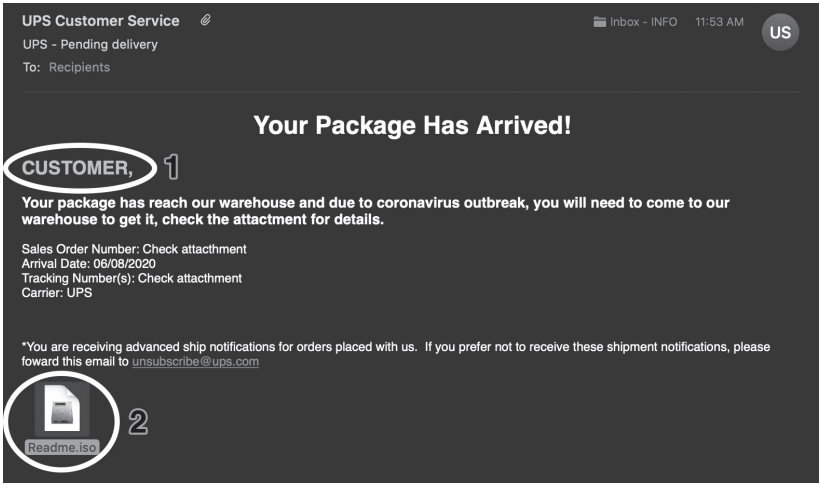
2. *Never reveal any personal information to any organization you do not know or trust.* Since there is no lottery and no prize, this scam email can generate revenue only by collecting as much information as possible and then selling it to other scammers. If you provide any information, expect to receive many more scam emails in the future.
3. This Euro Lottery email claims to originate in the United Kingdom. It mentions an office in Johannesburg, South Africa. It also references American Asia International Lottery as well. By trying to be as inclusive as possible, these scammers are casting a wide net to catch as many victims as possible around the world.



A SCAMMER PRETENDING TO BE PAYPAL:

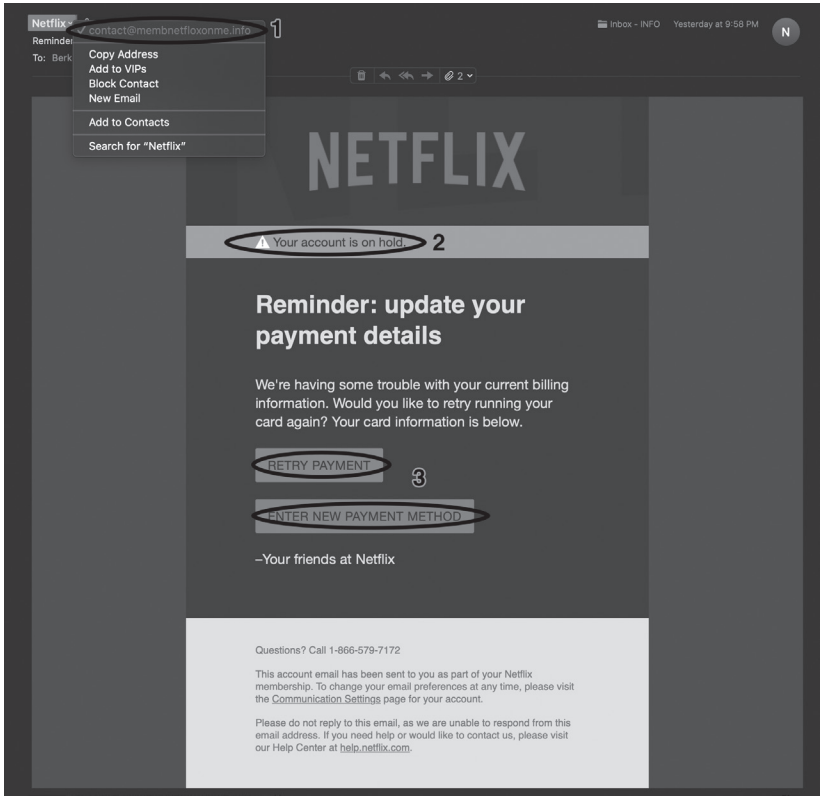
1. This email looks like it came from PayPal, but it really came from "me.saleshostn0-replay@wanjai.com." There are millions of emails in circulation that spoof PayPal. If you receive any email that claims to be from PayPal and you are not sure, simply forward it to spoof@paypal.com, and they will tell you whether it is legitimate or not.

2. Since PayPal knows the names and emails of all of its users, official emails would never address you as "Notice."
3. When the real PayPal includes buttons on the bottom of its emails, these buttons give a specific call to action, such as "Get the Details" or "Accept the Money." You should never click on any link in an email you were not expecting or you don't recognize, especially the supposed links for logging into an account.



A SCAMMER PRETENDING TO BE UPS:

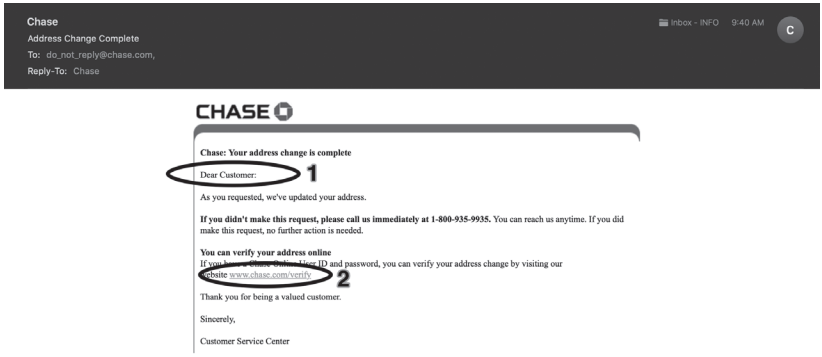
1. If you are a UPS customer, the company knows your name, address, and much more, so any legitimate communication from UPS will include your name.
2. Never click on any email attachments. “Readme.iso” is an executable file and is there only to install malware onto your computer. If you do click on it by mistake, simply close all pop-up windows and delete the email. Then run a scan with your antivirus software.



A SCAMMER PRETENDING TO BE NETFLIX:

1. If you glance at it quickly, "contact-membnetfloxme.info" might look like "contactmembnetflixme.info." While neither email address could be from Netflix, if the scammers can fool just one out of every one hundred thousand people, they are doing their jobs.

2. Scammers love to scare their victims into immediate action with ominous alerts and telling them their "account is on hold." Stop and think before you do anything. Is your Netflix working? Even if it's not working, that could easily be a coincidence. Log in to your Netflix account through the app or by typing the company's URL directly into your browser and check the status yourself.
3. Action buttons like these look like shortcuts to avoid unnecessary navigation to your Netflix account, but those buttons will not take you to the real Netflix website or your account. They will take you to a different website on a different server that is designed only to scrape (meaning steal) log-in credentials and sell them to the highest bidders. Always log in to your Netflix account the same way you have in the past, not by clicking a link in an email.



A SCAMMER PRETENDING TO BE CHASE BANK:

1. This looks like it could be a legitimate email from Chase Bank, but since I am not a Chase customer, I know it's more likely to be a scam than a mistake. If I were a Chase customer, though, I would know whether or not I made an address change. I could also simply log into my Chase account the same way I always do—without clicking on the link—and double-check any claims made in the email. And if I were a customer, Chase would know my name, so the "Dear Customer" is also a tipoff to a scam.
2. The URL www.chase.com/verify looks like a legitimate URL, but that doesn't

mean the link will take you to the indicated website. Any destination address can be assigned to any underlined URL as it appears. If you suspect the email is a scam or the address shown is not real, type it manually into your browser. If it is real, you will know soon enough, and if not, you just avoided a possible hack or scam.

Acknowledgments

The authors would like to thank the following people who helped make this book possible:

Gary Schober
Eileen Schober
Bill Schober
Ted Schober
Connell Rooney
Kelly Dwyer
Bill Dwyer
Every senior out there willing to try new technology, embrace the internet, and fight back against cybercriminals

All illustrations contained within this book were provided by Jake Thomas of www.JakeThomasCreative.com.

About the Authors

Scott N. Schober is the president and CEO of Berkeley Varitronics Systems (BVS), a forty-eight-year-old, family-owned company in New Jersey that designs and builds advanced wireless solutions and products for worldwide telecom and security markets. He is a cybersecurity and wireless technology expert, author, and host of a weekly video podcast entitled *What Keeps You Up At Night?* Scott's first book, *Hacked Again*, is a top-selling cybersecurity book and currently boasts over two hundred reviews (4.7 out of 5 star review average) on Amazon. *Hacked Again* chronicles his experiences as a hacking victim when BVS was hacked in 2013 and how he overcame those circumstances and shared his experiences to help others avoid being hacked. Scott's second book, *Cybersecurity*

Is Everybody's Business, was cowritten with his brother, Craig. In this industry-acclaimed book, the two authors focus on cybersecurity practices for small businesses and home offices that they have learned through years of running their own successful business.

Scott is a highly sought-after cybersecurity expert for media appearances on hundreds of news networks, including Bloomberg TV, *Good Morning America*, NPR, Bill O'Reilly, CNN, Fox Business Channel, CGTN, i24 News, News 12 NJ, and many more. Scott also regularly presents on cybersecurity best practices for small business and consumer protections at security conferences, including RSA, FutureCon, SecureWorld, ShowMeCon, and Cyber Investing Summit as a keynote speaker and panel expert. His expertise extends to such topics as the future of wireless technology, protection from insider threats, susceptibility to cyber breaches, the impact of drones, and distracted driving technology. You can learn more about him at www.ScottSchober.com.

Craig W. Schober is a writer, videographer, and the communications manager of Berkeley Varitronics Systems (BVS). In addition to his contributions to and edits of *Hacked Again* and *Cybersecurity Is Everybody's Business*, Craig creates all marketing content for BVS in the form of weekly blogs, white papers, website and e-commerce design and management, video podcasts, and viral video campaigns. Craig works closely with Scott as both a technical writer and video editor and has also worked in the film and video industry for the past twenty-five years, including as the writer, director, editor, and producer of his own award-winning feature films available on iTunes. He also happens to be Scott's younger brother.

Scott and Craig can both be contacted through www.bvsystems.com.