# Practical Cyber-Safety Tips

**M. E. Kabay, PhD, CISSP-ISSMP**
**Professor of Computer Information Systems**
**School of Business & Management, Norwich University**

## I. Reducing the Risk of Identity Theft

A. NEVER use a debit card for anything other than withdrawing money from an ATM. If crooks compromise your debit card number and PIN, they can withdraw money by wire from your bank account – and you are likely to be entirely responsible for the charges (no coverage from the bank).[1]

B. If you want to use your credit card for buying stuff on the Internet, establish a PayPal account. You register your card there but PayPal never reveals your card number to the merchants.[2]

C. ALWAYS sign up for immediate notification of all charges on your credit-card account. Find out if this service is available, and then have the notifications sent to your e-mail if you use that a lot or to your e-mail and your phone via SMS (text messaging) if you tend to prefer being notified by smartphone.[3] Check every charge immediately and call the security office at your card provider if you do not recognize the charge – like for example if it is a $700 invoice for escort services in Bangkok....

D. If you use online banking and credit-card maintenance, see if there is an additional security feature available such as requesting a security authorization code to be sent to your phone by SMS before you (or a thief) can log into your account.[4]

E. Check your credit-card and bank statements the day they arrive by mail or you can access them on your card's Website. Investigate anything you do not recognize.[5]

F. Identity thieves can use your name to establish loans – and then you are responsible for repaying them! Contact your bank to ask about *preventing* any unauthorized loan application in your name so that you are notified immediately to see if you authorize the loan.[6]

G. Look carefully at your ATM before putting your card into it. If there is a new piece of equipment that projects out of the surface of the device where you are supposed to put your card in, call the security office on the nearby phone – it may be a pirate card-reader that records or broadcasts your card information to criminals.[7]

H. If your credit card includes a choice for using RFID (radio-frequency identification), DON'T SIGN UP for RFID.

I. If you do use RFID-equipped cards, look into protective sheathing that will obstruct access to the information when you are not using the card. Unfortunately, though, the moment you take the card out of the sheath to use it, you will be vulnerable to RFID-snarfing by nearby criminals.

J. If you accept a credit-card-sized passport with RFID features, be careful to keep it in the foil-sheath to prevent the information from being collected by criminals overseas. Prevent yourself from being identified as a citizen of the US or Canada by surreptitious access to your passport information when overseas.

K. ALWAYS stand as close as you can to the keyboard of the ATM (automatic teller machine) you are using; do not let anyone "shoulder-surf" your PIN (personal identification number) from behind you. If someone gets within a couple of feet of you when you are entering codes into such a keyboard, either stop or, if you can swing it, tell the person politely to back away (you can say that close contact makes you nervous).

---

[1] (Schulz 2014)
[2] (Tips and Tricks HQ 2015)
[3] (Lowry 2015)
[4] (Awasthi 2015)
[5] (Pentagon Federal Credit Union 2014)
[6] (New Hampshire Department of Justice: Office of the Attorney General 2011)
[7] (Eddy 2016)

## II. Respond Immediately to Identity Theft

A. Be aware of the warning signs that you may be subject to identity theft < https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft#Clues >.[8]

B. If you receive information that your personally identifiable information (PII) has been compromised (e.g., by an online site such as AMAZON or by a company, non-profit, or government agency you have done business with), immediately take appropriate steps to prevent exploitation of your PII.

C. Use the instructions from the Federal Trade Commission's Website to respond to specific types of compromise < https://www.identitytheft.gov/Info-Lost-or-Stolen >.[9]

## III. Protect Your System Against Disaster

A. BACK UP your system regularly.[10] Copy all of your valuable files onto an EXTERNAL DISK DRIVE.

B. For important systems you care a lot about, daily "incremental" backups that store everything you have changed since the last incremental backup can be stored on your external drive.

C. DISCONNECT the external disk drive as soon as your backup is complete.

D. Store that backup device in a fire-proof safe if you have one or at least in a different room of your home or office. Lock it up if possible.

E. If you are using WINDOWS 7, 8, or 10, your system already has local backup available. You can use the **Control Panel | Backup and Restore** function to create a complete system backup – once a month is good.[11]

F. If you are using Apple systems, consider the iCloud function for automatic backup to external servers.[12]

G. A general and highly popular cloud-backup system is Carbonite.[13] It costs about $5 a month for unlimited storage.

## IV. Prevent Malware from Ruining Your System

A. ALWAYS run up-to-date, reputable antimalware (used to be called "antivirus") software. Highly recommended products from vendors such as AVAST, BitDefender, McAfee, Norton, Sophos, and others frequently reviewed in security publications update themselves frequently (sometimes several times a day) and silently to keep you protected against new threats.[14]

B. NEVER click on a popup that appears in your browser (e.g., Internet Explorer, Chrome, Opera, Firefox and so on) screen claiming that you have a virus or worm and that clicking will clean your system.[15] This kind of fraud is known as "scareware." Absolutely no legitimate company will EVER do such a thing – these popups are actually going to either (a) fake a terrifying FALSE report about hundreds of viruses on your system and ask you to pay LOTS of money to criminals or (b) install actual malware, including the dreaded ransomware.

C. Ransomware can strike anyone who is careless, but if you have proper backups you can ask a technician to wipe your system and restore all your files from your backups. You will be unable to replace whatever was encrypted by the ransomware after your last backup.[16]

D. NEVER click on an attachment (which may look like a file that is a DOCX, DOC, PDF, JPG, PNG, ZIP and so on) to an email that you are not expecting, even if it seems to be from someone you know. If it's unexpected and especially if the message doesn't instantly prove to you that it comes from your known contact (e.g., the message is completely generic, such as "You might like this," then contact the person you know using their own email address or phone number – don't just REPLY to what may be a fake email with harmful software in the attachment.

[8] (Federal Trade Commission nd)
[9] (Federal Trade Commission nd)
[10] (Kabay, Backups 2016)
[11] (Microsoft nd)
[12] (Apple 2016)
[13] (Carbonite, Inc. 2016)
[14] (PC Magazine 2016)
[15] (Davis 2016)
[16] (Vijayan 2016)

E. ALWAYS show file extensions on your system (e.g., DOCX, EXE etc.) and do NOT click on executables such as .COM and .EXE files unless you know for sure that they are safe.[17]

## V. Enable a Firewall on your System

A. Windows and Apple operating systems include firewalls that prevent hackers from entering your system. Be sure they are enabled.[18]

B. Some antimalware also includes firewall functions; consult a technical expert to decide which firewall to implement.

## VI. Use Good Passwords[19]

A. NEVER use the same password on multiple Websites.

B. By using a different random password for every Website, you prevent an attacker who discovers one of your passwords from opening many other Websites where you used the same password.

C. Generate random passwords that include uppercase and lowercase letters, numbers, and special characters (assuming the Website allows those). For example, you could create a password with random typing that looks like this: **j&Rn4Uy4k=a** for a particular Website.

D. You can use a free password generator online if you don't like random typing.[20]

E. ALWAYS use a password-safe function.[21] These products use one master password to encrypt all your other passwords for safety. They automatically type each Website's password when you need it. Certain browsers[22] and antimalware programs[23] have a similar password-protected master-password lists.

## VII. Don't Fall for Phishing Attacks[24]

A. NEVER click on a link in email from a stranger. Always hover your cursor over the link and look at the bottom of the screen to see exactly what the link points to. If it has weird elements such as large numbers of incomprehensible characters or numbers (e.g., http://bankofamerica.5793v.ru/%20ygheng8/wer089yv/bv3yhhna ) DO NOT CLICK ON IT! It is very likely a Website run by criminals.

B. NEVER respond to messages that claim to come from your bank, your hospital, your email provider and so on that claim that your account has been compromised and that you have to log in to a link in the message to provide your user information and password. If your password really were compromised, typing it would be meaningless. If you have any doubt about your account, log in yourself using the URL you already know and use. You can also call your bank (and so on) to ask about the message.

## VIII. Don't Fall for Email Frauds

A. NEVER communicate with a Nigerian prince, a Brazilian government official, or a Vietnamese bank official (and so on) who offer to put $23 million from abandoned money into your bank account so you can keep several million. These are "advanced-fee frauds" in which gullible people (idiots) agree to cooperate with people who have self-identified as criminals and who then suddenly announce that there's a hangup in the process and they need a few hundred dollars to get moving again. When the idiots agree and wire the money, the criminals turn around and ask for 10 times that amount the next time – and so on until the idiots finally realize they're being played for the fools they are.

B. NEVER do business with "companies" that send you unsolicited commercial email – the fact that they are doing that is evidence enough of their dishonesty. Don't buy anything from them, don't invest in wonderful offers, and don't sign up for free ANYTHING from companies you've never heard of.

---

[17] (Heng 2015)
[18] (Microsoft nd)
[19] (Kabay, Passwords: Compilation of Articles from Network World Security Strategies Newsletter 2016)
[20] (Strong Password Generator 2016)
[21] (Password Safe nd)
[22] (Opera 2010)
[23] (Bitdefender 2016)
[24] (Anti-Phishing Working Group 2016)

C. NO, you have not been given a large donation from a total stranger in Uganda who addresses you as Dearly Beloved and claims to be dying. It's another advance-fee fraud.[25]

D. NO, you have not won a lottery you never bought a ticket for.[26] The Irish Sweepstakes, the El Gordo Spanish lottery – these cannot offer you million-dollar prizes when you never registered for them – and in the US, it is ILLEGAL to participate in non-US gambling!

E. NO, you are not about to be arrested by the FBI for filing an incorrect IRS tax submission. Government agencies (police, tax collectors, inspectors…) NEVER communicate with people they are charging with a crime by sending an email announcement![27]

F. DON'T use the UNSUBSCRIBE function for any sender that you are not absolutely sure about. For example, if you sign a petition sponsored by a reputable organization (e.g., Amnesty International, National Wildlife Federation, and so on), you may receive a thank you note that includes a clear, obvious link for being removed. That link should be to the Website of the organization itself, not to a random-looking URL.

## IX. Don't Fall for Telephone Scams

A. NO police force will call you to announce that you are being arrested.

B. NO police call comes from Caller ID 911.

C. NO IRS official will threaten you by phone and insist that you immediately send a wire transfer to a company address.[29]

D. NO legitimate company will phone you to offer to extend your automobile warranty – these criminals will steal your money and provide no services.[28]

E. NO ONE can improve your credit rating magically by having you pay money to someone who phones you to offer that service.

F. If you receive a scary message by phone insisting that you log on to a "special Website" to fix a problem with your bank debit card or with your credit card, hang up and phone the regular number documented on your card to find out if there really is a problem.

G. NEVER continue your conversation with someone who sounds angry and threatening on the phone. Just hang up.

H. NO, Microsoft (or Apple) does NOT phone you to tell you have a virus on your system.[29] The person with the thick Indian accent is a criminal who wants to (a) log on to your system remotely; (b) install malware on it; and (c) demand payment for completely bogus "antivirus" or "technical support" services that sometimes go as high as $1,000. If you ever DO provide a credit card to pay for the fake services, the criminals instantly suck money out of your account up to the credit limit.

I. If your young nephew, niece, grandson, granddaughter or friend sends you a desperate phone call of poor quality claiming that they are in prison or kidnapped in a third-world country and need several thousand dollars to be set free, phone them at their home to find out; chances are, it's a fake call designed to trick you into sending money to crooks.[30]

## X. Don't Fall for Mail Fraud

A. NO, you will not earn large amounts of money for remailing products to other addresses. The criminals who trick victims into this scam are actually mailing products to innocent people who then forward them to members of the criminal ring. And the victims of this scam may be charged with federal crimes.[31]

B. No, you cannot earn $50,000 a year by visiting stores to evaluate them.

C. NO, you cannot be the winner of huge prizes at your local auto dealer by matching one of the numbers to a number concealed by wax you have to scratch off. Lots of the fliers have "winning" numbers – but they are solely to trick people into visiting the dealer with the bogus certificates.

D. NO, that official-looking printed sticker ("EXPEDITED DELIVERY" or "SECURE

[25] (Heuman 2011)
[26] (Australian Competition & Consumer Commission nd)
[27] (Hebert 2014)
[28] (Federal Communications Commission nd)
[29] (Federal Trade Commission 2014)
[30] (Unruh 2016)
[31] (U.S. Postal Inspection Service nd)

DELIVERY" or "PRIVATE" or "CONFIDENTIAL" on the envelope you have received that has no return address on the front or back is NOT from the US Postal Service. It's designed to look official but actually suggests that the senders are trying to trick you into something fraudulent.

## XI. Don't Fall for Rumors

A. NEVER believe or forward an alarming story you've received from a friend or read on a social media without checking it on SNOPES.COM.[32]

B. NEVER forward ANYTHING that includes promises, threats or warnings about failing to forward the message: these are chain letters and they are all nonsense.

C. Microsoft does NOT and cannot keep track of whether you forward a message, and they certainly do not hand out free prize money for forwarding email, contrary to the claims that you will see in some chain letters.

## XII. Use Email Properly[33]

A. NEVER put lists of people in the TO or CC field of an email message you are writing unless (a) it is essential that everyone see who is receiving the email; and (b) they have all agreed to have their email addresses made known to everyone else.

B. NEVER use REPLY ALL unless there's a good reason to. If you receive an announcement from your synagogue or department chair in which there are 52 addresses in the TO or CC field, don't write "Thanks" and REPLY ALL: 51 other people than the sender are going to see your response for no good reason.

C. DON'T leave copies of copies of copies of copies of copies of old messages in your reply. Delete the old useless stuff, keeping only a specific quotation if necessary.

D. Don't send a link to someone without at least a bit of text that demonstrates that the message is really coming from you. Use a recipient's nickname, include a warm greeting obviously from you, refer to a recent event or conversation, and so on.

[32] (SNOPES 2016)

[33] (Kabay, Using Email Safely and Well (v8) 2016)

**Works Cited**


Anti-Phishing Working Group. 2016. "APWG -- Unifying the GLobal Response to Cybercrime." *APWG*. Accessed May 22, 2016. http://www.antiphishing.org/.

Apple. 2016. "iCLoud Support." *Apple*. Accessed May 22, 2016. https://www.apple.com/support/icloud/backup-storage/.

Australian Competition & Consumer Commission. nd. "Unexpected prize & lottery scams." *SCAMWATCH*. Accessed May 22, 2016. https://www.scamwatch.gov.au/types-of-scams/unexpected-winnings/unexpected-prize-lottery-scams.

Awasthi, A. 2015. "Reducing Identity Theft using One-Time Passwords and SMS." *EDPACS: The EDP Audit, Control and Security Newsletter*. Dec 21. Accessed May 22, 2016. http://authentictechs.com/wp-content/uploads/2013/12/EDPACS.pdf.

Bitdefender. 2016. "How to use the Bitdefender (2014) Wallet." *Bitdefender*. Accessed May 22, 2016. http://www.bitdefender.com/support/how-to-use-the-bitdefender-(2014)-wallet-1202.html.

Carbonite, Inc. 2016. "The #1 Choice in Backup." *Carbonite*. Accessed May 22, 2016. https://www.carbonite.com/en/cp/backup.

Davis, P. 2016. "How to Recognize a Fake Virus Warning." *Business Know-How*. Accessed May 22, 2016. http://www.businessknowhow.com/security/scareware.htm.

Eddy, M. 2016. "How to Spot and Avoid Credit Card Skimmers." *PC Magazine*. Apr 5. Accessed May 22, 2016. http://www.pcmag.com/article2/0,2817,2469560,00.asp.

Federal Communications Commission. nd. "Beware of Auto Warranty Scams." *For Consumers*. Accessed May 22, 2016. https://www.fcc.gov/consumers/guides/beware-auto-warranty-scams.

Federal Trade Commission. nd. "Report identity theft and get a recovery plan." *IdentityTheft.gov*. Accessed May 22, 2016. https://www.identitytheft.gov/.

—. nd. "Spam." *Consumer Information*. Accessed May 22, 2016. https://www.consumer.ftc.gov/articles/0038-spam.

—. 2014. "Tech Support Scams." *Consumer Information*. Jan. Accessed May 22, 2016. https://www.consumer.ftc.gov/articles/0346-tech-support-scams.

—. nd. "Warning Signs of Identity Theft." *IdentityTheft.gov*. Accessed May 22, 2016. https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft.

Hebert, A. 2014. "Scammers continuing to pose as IRS agents." *Federal Trade Commission Consumer Information*. May 29. Accessed May 22, 2016. https://www.consumer.ftc.gov/blog/scammers-continuing-pose-irs-agents.

Heng, C. 2015. "How to Force Windows Explorer to Always Show You the File Extensions." *Howtohaven*. Accessed May 22, 2016. http://www.howtohaven.com/system/show-file-extensions-in-windows-explorer.shtml.

Heuman, E. 2011. "[Te-banned] ~*~ [spam] Dearly Beloved." *VMware*. Jun 21. Accessed May 22, 2016. http://lists.vmware.com/pipermail/te-banned/2011-June/000003.html.

Kabay, M. E. 2016. "Backups." *M. E. Kabay*. May 22. Accessed May 22, 2016. http://www.mekabay.com/infosecmgmt/backups.pdf.

—. 2016. "Passwords: Compilation of Articles from Network World Security Strategies Newsletter." *M. E. Kabay*. May 22. Accessed May 22, 2016. http://www.mekabay.com/infosecmgmt/passwords.pdf.

—. 2016. "Using Email Safely and Well (v8)." *M. E. Kabay*. Jan 16. Accessed May 22, 2016. http://www.mekabay.com/infosecmgmt/emailsec.pdf.

Lowry, E. 2015. "Consumer Watchdog: Setting Up Credit Card Transaction Text Message Alerts." *Magnify Money*. Mar 15. Accessed May 22, 2016. http://www.magnifymoney.com/blog/consumer-watchdog/consumer-watchdog-setting-credit-card-transaction-text-message-alerts666220981.

Microsoft. nd. "Back up your files." *Microsoft Windows*. Accessed May 22, 2016. http://windows.microsoft.com/en-us/windows/back-up-files#1TC=windows-7.

—. nd. "Turn Windows Firewall on or off." *Microsoft*. Accessed May 22, 2016. http://windows.microsoft.com/en-us/windows-10/turn-windows-firewall-on-or-off.

New Hampshire Department of Justice: Office of the Attorney General. 2011. "Consumer Sourcebook: Identity Theft." *New Hampshire Department of Justice: Office of the Attorney General*. Accessed May 22, 2016. http://doj.nh.gov/consumer/sourcebook/identity-theft.htm.

Office of the Comptroller of the Treasury. nd. "Advance Fee Fraud." *U.S. Department of the Treasury.* Accessed May 22, 2016. http://www.occ.treas.gov/topics/consumer-protection/fraud-resources/advance-fee-fraud.html.

Opera. 2010. "Forms: Password Manager." *Opera Software.* Accessed May 22, 2016. http://help.opera.com/Mac/10.50/en/wand.html.

Password Safe. nd. "Password Safe." *Password Safe.* Accessed May 22, 2016. https://pwsafe.org/.

PC Magazine. 2016. "Antivirus Software." *PC Magazine.* Accessed May 22, 2016. http://www.pcmag.com/reviews/antivirus.

Pentagon Federal Credit Union. 2014. "How to review my monthly credit card statement." *PenFed Credit Union.* Jun 4. Accessed May 22, 2016. http://blog.penfed.org/review-monthly-credit-card-statement/.

Schulz, M. 2014. "The Debit Card Danger You're Probably Forgetting: Paying with a debt card is much riskier than swiping your credit card." *U.S. News & World Report.* Sep 22. Accessed May 22, 2016. http://money.usnews.com/money/blogs/my-money/2014/09/22/the-debit-card-danger-youre-probably-forgetting.

SNOPES. 2016. "Snopes Home Page." *Snopes.com -- Rumor Has It.* May 21. Accessed May 22, 2016. http://www.snopes.com/.

Strong Password Generator. 2016. "Strong Password Generator." *Strong Password Generator.* Apr 8. Accessed May 22, 2016. http://www.strongpasswordgenerator.org/.

Tips and Tricks HQ. 2015. "7 Advantages to Using PayPal to Buy Online." *Tips and Tricks HQ.* Mar 6. Accessed May 22, 2016. https://www.tipsandtricks-hq.com/7-advantages-to-using-paypal-to-buy-online-2668.

U.S. Postal Inspection Service. nd. "Reshipping fraud." *USPIS.* Accessed May 22, 2016. https://postalinspectors.uspis.gov/radDocs/consumer/ReshippingScam.html.

Unruh, Bob. 2016. "Kidnapping scam explodes across America." *WND.* Feb 2. Accessed Jul 16, 2016. http://www.wnd.com/2016/02/kidnapping-scam-explodes-across-america/.

Vijayan, J. 2016. "Here's How To Protect Against A Ransomware Attack." *Information Week Dark Reading.* Feb 4. Accessed May 22, 2016. http://www.darkreading.com/endpoint/heres-how-to-protect-against-a-ransomware-attack/d/d-id/1324169.