Bruce Berls

708 Gravenstein Hwy N PMB 180
Sebastopol, CA 95472
(707) 703-1601
bruceb@bruceb.com
www.bruceb.com

Rules for Computer & Online Safety 2018

Email & online security	Computers	Phones & tablets
Antivirus programs	Adware	Passwords
Social networks	Phone scams	Wire transfers

These are the rules for computer and online safety in 2018.

You will be safe if you are cautious. Stop and think before you click on links, before you call unfamiliar phone numbers, before you install programs, and before you fill in passwords. Only your vigilance will protect you against bad guys.

Do not click on links in email messages unless you are *100% certain* they lead somewhere you want to go.

We are being assaulted by a torrent of phony email messages from criminals. The messages look legitimate. The links lead to fake websites that will try to steal your password or credit card number.

If you fill in your password or credit card number on a fake login screen, the bad guys will capture it.

If you click on a link to a poisoned website and your computer is not up to date, the bad guys will install viruses on it.

Only your paranoia can protect you.

Always hover over a link before you click on it. Do not click unless it is obviously a legitimate link.

When you hover over a link, a popup will show you where it leads. Don't click if the link doesn't match the company that you expect. If it is a shortened link and you can't tell where it goes, assume it is suspicious.

If you get a malware message by email and you don't click on a link, it hasn't hurt your computer. Delete it.

Do not click on a link to a file in Google Drive, Dropbox or other online services unless you know with *100% certainty* that the file is something you want.

The latest attacks appear to be a link in an email message to a PDF or other online document. The links lead to poisoned websites or fake login pages that will capture your password for the bad guys.

Never, never, *never* open email attachments unless you know with *100% certainty* that the attachment is something you expected and want to receive.

This is important. Email attachments are still the primary method of spreading viruses and ransomware. If you open the wrong Word document or PDF, you can take down your entire company. Don't open email attachments!

Just because something is listed in a Google search doesn't mean it is safe.

Make a judgment about where you're going *before* you click.

Back up your computers.

Choose a backup strategy, understand how it works, and keep your backups up to date.

An online backup is the best choice for most people. It increases the chance of a full recovery if a ransomware virus gets on your computer and destroys your files.
Examples: Backblaze, IDrive, Carbonite, Mozy, B ruceb Cloud Backup.

You may also want to have a local backup to an external hard drive or NAS. Windows 10 users can use File History.

If your computer displays a message while you are browsing the Internet claiming that you have been hacked or infected with a virus, it is a lie by criminals.

Your computer is not infected with anything and you did nothing wrong. If you cannot close the window, close the browser window with task manager or shut down your computer by holding the power switch in for 15 seconds. If the message reappears after you restart, contact your regular IT support for help.

Do not call the 800 number for "tech support."

You are calling criminals who will lie to you.

If you call the 800 number and give them a credit card number, you will be charged hundreds of dollars for nothing.

The card number is effectively stolen and you will have to cancel it.

If you call the 800 number and give them remote access to your computer, you can never trust that computer again, no matter how thoroughly it is cleaned.

You will have to wipe it out and reinstall everything from scratch. If your personal information is stored on the computer – passwords, tax information, bank account info, social security number, etc. – you should consider taking steps to protect yourself against identity theft. That might include a fraud alert in your credit report, freezing your credit report, and monitoring your credit report and financial accounts for unauthorized activity.

Set a PIN code, password, or fingerprint authentication to unlock your phone or tablet.

Smartphones and tablets are easily misplaced or stolen.

Review the apps on your phone to see if they have permission to do anything unnecessary.

Apps on your phone may have permission to use the microphone or camera, to track the phone's location, to access your contacts, or to send SMS messages. Legitimate, well-known apps will use those permissions responsibly. Malicious apps can abuse those privileges and might be monitoring your activity or selling your personal data. Periodically look at the apps on your phone; uninstall the ones that aren't important and turn off permissions that don't seem to be necessary.

On Android, go to ***Settings / Apps & notifications / App permissions***. You can group apps by permission and disable a permission for an app if appropriate.

On iPhones and iPads, go to ***Settings / Privacy***. You can choose each permission and disable it with the slider.

Do not keep confidential or privileged information on a mobile device in an unprotected app.

Run antivirus software on your computer.

Windows 10 has built-in security protection, Windows Defender. Windows 7 users should use Microsoft Security Essentials. There are also security programs from Norton, McAfee, and others, of course, but they are not recommended; most of them are poorly written and cause more problems than they solve. Many IT professionals suggest periodic scans with Malwarebytes as a supplement to Windows Defender/Security Essentials.

Antivirus software barely slows down the bad guys.

They've been finding ways to avoid it for 20 years. Use your common sense. Be cautious when clicking on links. Don't open unexpected email attachments. Read and think before you click OK.

Know the name of your security software.

If you get a "security warning" that does not display the exact name of your security software, it is phony; if you click on anything, you will probably install malware.

Don't download "free" programs or add unnecessary browser extensions.

Adware is distributed with "free" games, PDF programs, media players, and even with quite legitimate utilities like Java and Adobe Reader. Your security program will not stop you from installing adware, but adware can bring down your computer just as thoroughly as malware from bad guys.

Do a custom install of any new program and decline unnecessary extra software.

When you're downloading and installing a program – especially a free program – scrutinize every screen that comes up. Look for checkmarks that can be unchecked. Look for weasel words that might conceal a disclosure that other programs are coming along. Always do a custom install and study the options.

Choose passwords carefully.

Your passwords are your defense against identity theft, financial loss, compromised computers, and breaches of confidentiality and privilege. If you use a weak password, or if you use the same password over and over every time something calls for one, you are jeopardizing yourself and your business.

Use a different password for every site.

When large companies are hacked, the bad guys immediately test hacked passwords on other sites in case you used the same one somewhere else. There is a tip here for creating unique passwords that you can remember.

Use a password manager for your online passwords.

LastPass is the best known password manager. It is free and secure. If you're not already using LastPass, spend time learning about the program and how it works.

If you are a LastPass user, periodically run its Security Check and update any weak and duplicate passwords.

Set up Lastpass emergency access for a trusted family member.

Consider using two-factor authentication.

Two-factor authentication combines a password and a second check, typically a code sent to your phone in a text message or a number generated by an app on your phone. Many services are adopting two-factor authentication and it drastically improves security. It's more difficult to use than a simple password, but it's much less trouble than being hacked.

Review the apps connected to your online accounts.

You have probably used your online accounts to sign up for apps and web services. Those apps and services may still be connected to your personal data and selling it to advertisers or worse. Periodically go through the list and disable any that aren't necessary.

Facebook – click on ***Settings / Apps***

Twitter – click on ***Settings & privacy / Apps***

Google – go to the Google Account page, then click on ***Sign-In & Security / Apps with account access***

Microsoft does not call to fix your computer.

There is a resurgence of fraudulent phone calls from criminals trying to steal your credit card and install malware on your computer. The scammers play on our fears about online security, just like the poisoned web pages that bring up phony onscreen security warnings. Don't lower your defenses!

Don't answer the phone if you get a robocall.

If you don't recognize the caller or the phone number, don't pick up. If you pick up, the number will be marked in the robocaller's database as belonging to a live person and you'll get more calls. If the voice message says to pick up and press a number to be put on the Do Not Call list, do not pick up and press the button. They're lying about the Do Not Call List.

If you answer the phone and there's a pause of half a second or so, hang up.

The call is almost certainly from a scammer or telemarketer; the pause happens as the automated dialer hands off the call to a person in a cubicle.

If you answer the phone and it turns out to be a scammer or telemarketer, hang up.

Don't say another word. Don't engage them. Don't tell them they should be ashamed. Don't explain why you're hanging up. Don't teach them a lesson by putting them on hold so their time is wasted. Don't yell at them through a megaphone to hurt their ears. Don't say *any* unnecessary words. Just hang up. You won't hurt their feelings. They're not judging you.

Do not approve a wire transfer without verbal authorization.

One of the worst scams for businesses starts with a *targeted email*. Bad guys research your business and craft a fake email asking the CFO to send a wire transfer. The request will appear to be legitimate. The bad guys might register a confusingly similar domain name to carry out the scam. They'll intercept email and send responses that appear to be legitimate. If you authorize a wire transfer to bad guys, you have no recourse against the bank – and the bad guys are long gone with the money, of course.

Educate employees about the risk of wire fraud phishing schemes.

Set up a strict business protocol that a wire transfer cannot be approved without verbal authorization from someone known to the person approving the transfer.

There's more info about the wire transfer scam here.

Be careful out there!