EBOOK

backupify
a datto company

The IT Admin's Checklist **for Complete Office-Wide Computer Security**

What Today's Admins Can Teach Users To Keep Them Safe

COMPUTER SECURITY VS. COMPUTER USERS

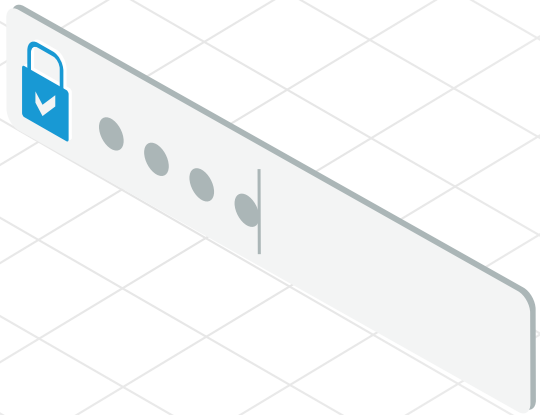
Information Technology administrators know the value of computer security. Communicating that value to your end users, however, can often prove to be a challenge.

Remember, every security best practice is a trade-off between convenience and safety. Users who don't understand the stakes involved in computer security won't often give up their convenience. Below are seven key aspects of computer security that all IT admins should teach their users.

These sections are arranged to describe computer security from the inside out, starting with strong passwords and moving through email and web browsers to workstations, mobile devices, whole networks and even your entire work and social environment. They describe simple computer security best practices and why they are important -- in plain, non-technical language most users can understand.

HOW CAN I USE THIS RESOURCE WITH MY USERS?

Here's how: You can and should share each of the sections below directly with your users to stress the basics of security. At the end of each section is a wrap-up highlighting the key bullet points. Bonus! At the very end of this ebook we have an easy to use checklist to pass directly on to your end users.



PASSWORD SECURITY

No One Needs Your Password, Ever

Here's an easy way to tell if someone is trying to steal information from you, or do damage to your technology: They ask for your password.

No person ever needs your password. Not your boss. Not your co-worker. Not the tech support lady on the phone or the repair guy standing over your laptop. Nobody needs your password.

Any of the people who legitimately need to access your system can get in without your password. They have privileges on your system necessary to their jobs, and they can get into your account without your password.

The only reason someone needs your password is to fool a computer or an online service into thinking they are really you. That's not legitimate behavior. Don't give out your password.

"But what about those websites that say I can log in with Facebook or Google?" Those websites don't ask for your password. They send you to a pop-up window on Google or Facebook or Twitter, and you can enter your username and password into Google, Facebook, or Twitter on those actual websites. Then, Google or Facebook or Twitter send an encrypted bit of code called a token that tells the website who you are, but doesn't tell the website your password. Basically, Google or Facebook or Twitter is vouching for you so you don't have to give your password to a stranger. No websites should give out your password.

Don't give out your password, to anyone or anything, ever.

Long, complicated passwords are harder to guess, but are also harder to remember. That's why you shouldn't use a password; **you should use a passphrase.**

Use a Passphrase, Not a Password

You're really bad at picking passwords. Don't worry, most people are. In fact, hackers can usually guess your password because most people pick really common, really simple, really insecure passwords. Passwords like 123456 and, well, password.

Short passwords that contain obvious words are easier for hackers to guess. Hackers can simply try any of the most common passwords first and, if that fails, they just use a program that tries random words or common sequences of numbers. When that fails, hackers try random series of letter and numbers.

The longer and less common your password, the harder it is for hackers to guess. Most people choose short, simple, obvious passwords because they are easy to remember. Long, complicated passwords are harder to guess, but are also harder to remember. That's why you shouldn't use a password; you should use a *passphrase*.

A passphrase is a short sentence that's easy to remember but, hopefully, is hard to guess. So, for example, instead of using your daughter's birth date as a password, use 'I love my baby girl 4-ever' as a passphrase. You probably can't remember a 16-digit random string of numbers and letters, but you can remember that you'll always love your little girl (and that you used a funky number and punctuation combo to spell forever).

And, best of all, hackers won't be nearly as likely to guess your passphrase.

Use Two-Factor Authentication Wherever You Can

Even if you don't give out your password and you use a good passphrase, it's really only a matter of time before a hacker gets ahold of your password. Hackers steal millions upon millions of passwords every year—through no fault of the users that lose them.

SHARE THIS

Password security wrap-up

1. Don't share your password with anyone
2. Use a passphrase instead of a password
3. Combine your passphrase with two-factor authentication

That's why you need a second line of defense: two-factor authentication.

Think of your password as a key that unlocks the door to your computer and your online accounts. If someone steals that key, they can unlock that door and walk into your system, stealing or wrecking anything inside.

Two-factor authentication is like installing a deadbolt lock above the lock already in your computer's door—a deadbolt that uses a different key from the door itself. Thus, if a hacker wants to get inside your computer, they would need to steal two different keys.

Where the analogy breaks down is that two-factor authentication isn't about using two different passwords. Two-factor authentication uses a password and then some other piece of information stored separately from your password.

For example, many modern laptops include fingerprint readers, which require you to enter a password and scan your forefinger or thumb to access the system. Services like Gmail or Twitter can send special codes to your smartphone—either by voice call, text message or through an app—which you must combine with your password to log in.

With two-factor authentication, a hacker has to do more than steal a list of passwords from a server somewhere to hack into your computer. Hackers would need to steal your password and physically steal your smartphone (or your thumb) to get into your computer, and that is far, far less likely.

EMAIL SECURITY

Don't Act On Mail Content From People You Don't Know

Here's a funny thing about email—I can send you an email even if I don't "know" your email address. Once a hacker (or a shady marketer) finds an email from anyone at your company, odds are they can figure out how email accounts are "named" where you work.

For example, if someone gets ahold of an email from your sales manager John Doe, and his email is jdoe@yourcompany.com, it's pretty obvious that your company uses "first initial, last name" as the naming system for its email accounts. From there, hackers can guess the email of anyone they know (or suspect) works at your company.

The worst thing you can do is confirm those guesses.

If you reply to a suspicious email, the hacker knows the email address works. If you open any attachment, or click on any link, or even download any image included in a strange email—because lots of good mail programs block the images that are included in emails, and you have to "click here to download images"—the hacker now knows that this email address is real and that there's a person they can hack (or con) on the other end.

It's perfectly okay to open an email from someone you don't know, and it's perfectly safe to read it. But unless you're really sure that the email is legitimate, don't act on it. Don't reply, don't click, and don't download. To do otherwise is to make yourself a target.

For more IT admin tips, subscribe to the Backupify blog

SUBSCRIBE

Don't Open Attachments You Haven't Scanned

Okay, let's say you're pretty certain the email you just received is legitimate, and it has an attachment included with the email that you want to open. You need to scan the attachment first.

Your computer has an antivirus scanner on it. (Or, if it doesn't, go yell at your IT administrator for falling down on the job.) Odds are, you can right-click on any email attachment before you download it, or at least before you open it, and there will be an option to use your security scanner to check if the attachment is safe.

Email attachments are the easiest way for hackers to infect your computer—and your company—with malicious software. Always scan email attachments before you open them—even in emails from people you know.

Just because that email appears to be from your sales manager John Doe, that doesn't mean it's really from him. Hackers can "spoof" email addresses to make them look like they came from someone else. Hackers could also have hacked John's email account and are using it to send dangerous attachments. Or—and this is very common—John could simply be a lot less careful than you are and he is unknowingly passing around an infected attachment, putting everyone else at risk.

A wise man once said *trust, but verify*. No matter who sent you an email attachment, scan it before you open it. It's always better to be safe than sorry.

Verify Links in Emails Before You Click Them

Just like email attachments, links in emails need to be checked before you open them. Websites can be "spoofed" just as easily as email addresses, but fake websites are also much easier to notice if you know what to look for.

SHARE THIS

Email security wrap up

1. Don't respond to email from strangers
2. Don't open any attachments you haven't scanned
3. Don't open any links you haven't checked
4. Always back up your email

Let's say, for example, someone sent you a link to a news story from The Chicago Tribune. First, you need to make sure the link actually points to The Chicago Tribune. If the sender formatted the email to hide the link—or example, you need to click some text like click here or check this out—you should check to see what the actual web address is before you click on the link.

If you hover your cursor over the linked text and wait a moment, most mail programs or web browsers will show a small pop-up—either directly over the link or at the bottom of the screen—which tells what web address the link is pointing to.

Always check your links before you click on them!

In our example, the web address should include chicagotribune.com somewhere inside the link. There should be no text or symbols between chicagotribune and .com. Hackers often confuse their victims by creating web addresses that look like real websites, but are actually part of a different site altogether.

For example, hackers might create a fake website called newssource.com and then make it look like The Chicago Tribune by creating a web address like chicagotribune.newssource.com. At first glance, it looks like you're going to the Tribune's web site, but you're actually going somewhere on newssource. com.

Even if the web address is fully spelled out in the body of the email—for example, it says http://www. chicagotribune.com—hover over the link to be sure it's actually going to chicagotribune.com. Often times, it isn't. If a link points somewhere other than where it should, or the address looks unusual, don't click on the link.

Again, when it comes to email security, it's better to be safe than sorry.

WEB BROWSER SECURITY

Don't Click "Yes": Install from Safe Sources Only

When you see a message in your web browser that tells you to install anything, stop. That app that offers to save you time, money, or let you view a video might be malware, as in software designed to do damage or help out hackers. Check with your IT advisor to obtain their approval before you install anything from your web browser.

Once you've received the "OK", only install items from safe sources: the vendor's download site or your browser's add-in store. For example, if you must install Adobe Flash, type www.adobe.com and navigate Adobe's web site to download Flash directly from Adobe. That way, you know the website hasn't been spoofed.

The same is true for browser extensions and plug-ins. Install add-ons and extensions only from the official browser sites: iegallery.com for Internet Explorer, chrome.google.com/webstore for Chrome, addons.mozilla.org for Firefox, and extensions.apple.com for Safari.

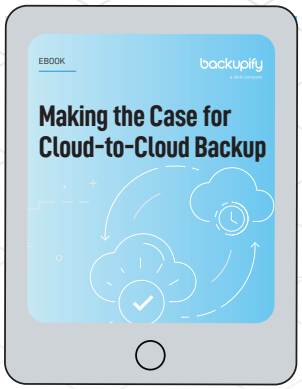
Look for the Lock

Look for a lock icon before you enter information or place an order on a website. Most modern browsers display a green padlock to indicate a secure connection between your browser and the site you're visiting. If you don't see the indicator, don't share any information.

(Learn more about the browser security indicator for your browser: Internet Explorer, Chrome, Firefox, and Safari.)

After you enter your username and password for a site, most browsers ask "Would you like to store this password?" **While that may be convenient, such a practice isn't secure.**

You may also be interested in:



Making The Case For Cloud-to-Cloud Backup
DOWNLOAD NOW

Save and Sync Selectively

After you enter your username and password for a site, most browsers ask "Would you like to store this password?" While that may be convenient, such a practice isn't secure—especially since not all browsers encrypt the information stored on your system. You're safer to decline such an offer. Instead, use a password manager program that encrypts your stored logins and passwords.

(Learn more about password managers and additional ways to secure your accounts here.)

Similarly, most modern platforms and browsers allow you to sync your settings to various devices. Log into a browser (or device), allow it to sync, then you'll have access to your saved sites and bookmarks, your browsing history, and your settings. Allow this sort of sync only on devices you fully control in a secure location. (It's fine to sync your personal workstation at the office and your personal tablet at home. It's not okay to sync with the computer in the lobby of the hotel or at a kiosk at a trade show.) For maximum security, don't allow this sort of sync—ever.

(Learn more about sync capabilities for Windows, Apple iCloud, Chrome, and Firefox platforms.)

If You Log On, Log out

Do this one exactly as it reads: if you log in to a website, log out when you leave. Visit Facebook.com? Log in. When you're done visiting Facebook…log out. The same is true for every site you visit: when you place an online order, update your organization's database, or join a web meeting. When you're done, log out.

SHARE THIS

Web browser security wrap-up

1. Only install from safe sources
2. Look for the lock
3. Save and sync selectively
4. If you log in, log out
5. Clear and back up everything

In some cases—think, Gmail—you might stay logged in during the day, then log out when you leave. In other cases—like Amazon.com—log in to order an item, and then log out. When you log out, you improve security: no one can sit down at your computer and access your account without your login (unless you saved your username and password, which is why we told you not to do that).

Clear and Back Up Everything

Finally, you can always delete browser information. Internet Explorer, Chrome, Firefox, and Safari all provide methods to delete or reset locally stored info like passwords, mailing address and phone numbers. These methods only clear profiles and settings for the browser—they don't impact files you've downloaded and stored elsewhere. Also, be aware that a browser reset can't clear information that other computers have stored about your activity. Your activity may still be stored by the sites you've visited, or by monitoring tools elsewhere on your network. Just because your local copy of Internet Explorer forgot what you were browsing on Amazon doesn't mean Amazon forgot—or will ever forget.

A computer or smartphone that never connects to a network will be more secure, but a disconnected system is also not very useful. A network connection presents an inherent risk: browse to the wrong site, hit "enter" too quickly, and your browser could be infected with a virus or hacked. Make sure to back up your data so that you can quickly recover and resume work if that happens.

SMARTPHONE SECURITY

Every Smartphone or Tablet Has a Lock Screen. Use it. Always.

Your smartphone or tablet is designed for quick, easy access to all your data. No one wants to have to log into their Gmail inbox or Facebook account on the go—much of the value of a smartphone is that it can stay logged into these services and notify as soon as your receive a message or an update—so smartphone versions of these apps let you stay logged in for weeks at a time. In many cases, the same thing is true for your personal banking app or the app you (almost never) use from your insurance company.

This means that anyone who gets ahold of your phone can probably read your email, raid your bank account and maybe even scroll through medical history without ever needing to know a single username or password.

This is why your smartphone or tablet has a lock screen—the setting that makes you punch in a PIN number or connect a pattern of dots before you can use your phone. It's not just there to be annoying; it's there to keep a pickpocket (or your kids) from snatching your phone—and thereby viewing or stealing everything important in your life that connects to your phone—all in one fell swoop.

If you don't want to spill all your personal secrets, get robbed, or have your identity stolen, use your phone's lock screen. Set it to turn on the moment your device is idle. Always.

Nobody Should Borrow Your Smartphone, Ever

Your smartphone's lock screen can't keep you safe if you turn it off whenever someone asks. This is one of the oldest tricks in the book: ask to borrow someone's phone to make a call, and then step away for "privacy." What appears to be a simple act of kindness is the easiest way for someone to read your emails, texts, calendar or any other private list or personal information kept on your phone.

SHARE THIS

Smartphone security wrap-up

1. Always use a lock screen
2. Nobody borrows your smartphone
3. Don't respond to texts from strangers
4. Don't answer calls from strange phone numbers
5. Back up everything

Here's a quick tip: if you wouldn't let someone borrow your wallet, they shouldn't be allowed to borrow your smartphone or mobile device.

Text Messages Follow the Same Dos and Don'ts as Email

Everyone has heard a raunchy comedy routine about the jealous spouse who wants access to your text message history to see if you've been cheating. What's interesting is that so many of us innately understand the privacy issues around text messages, but fail to realize that text messages are just another version of email you get on your phone.

Just as with email, you shouldn't accept gifts from strangers.

Don't reply to texts from people you don't know. (Not even the old "reply S to stop these messages.") Don't follow links in texts from people you don't know. Don't download pictures or video or any other files via text from people you don't know. That's a great way to get your phone hacked.

If you don't recognize the number, just delete the text and move on.

Phone Calls Follow the Same Dos and Don'ts as Email

Here's where many of us drop the ball on smartphone security: actual live voice calls. Odds are, the mobile number you have today was a mobile number five, 10 or even 20 years ago. (Yes, mobile phones are that old.) Con artists and hackers can buy or steal lists of mobile phone numbers and randomly dial them to see who is gullible enough to answer. Once you've answered, the hacker knows that the number is still in use and that the phone belongs to someone who'll answer calls from strangers.

Welcome to the shortlist for future scams and hack attacks.

(The dialing software can detect when voicemail answers a call, and the scam artists drop off to avoid paying call charges as soon as they can. Letting the call roll to voicemail is pretty safe. If the call is from a legitimate person with a number you don't recognize,

they'll leave a message that identifies themselves and you can call them back.)

Again, if you don't recognize the number, don't answer. Let voicemail handle it.

Back Up Everything On Your Smartphone Or Tablet

Android smartphones and tablets, iPhones and iPads all have basic backup systems. Lose your phone, and more or less all the contacts and pictures you saved on the device can be downloaded from Google or Apple. That is, if you have those backup settings turned on. Lesson one is make sure you have all the backup features available for your phone turned on

WORKSTATION SECURITY

Use an Active Security Suite

A "security suite" is what computer nerds call an antivirus program, mostly because a security suite does a whole lot more than antivirus software ever used to do. Security suites protect your system from viruses—and malware, spyware, and network attacks. Not all malicious programs are viruses. Some programs present themselves as useful, but are spyware. For example, a program that offers to alert you to discounts or deals, but also secretly monitors everything you do online. Your security suite should detect that and disable these kinds of software.

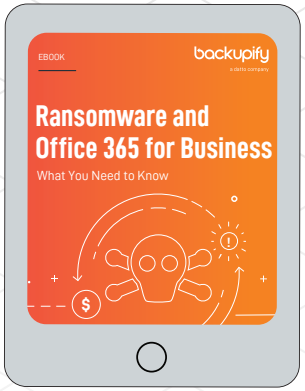
If you use a company-owned system, your IT folks likely provide a security suite. You should make sure that this security software is running and active. If it isn't, turn it on and immediately run a full system scan.

Update your Software

Keep your operating system, security suite, and programs up-to-date. Microsoft releases patches on the second Tuesday of each month. If you update your own system, check then. If an IT professional manages your updates, they may test

Applications—**especially programs that connect to the internet**—also offer a way for attackers to access your system.

You may also be interested in:



Ransomware and Office 365 for Business: What You Need To Know

DOWNLOAD NOW

Microsoft's patches before they deploy the patch to your system, so there may be a delay.

Many security suite vendors release updates every few hours. Your system should receive and apply those automatically to protect against recently identified threats. It can occasionally prove annoying when your system demands to be restarted or slows down because it is automatically applying these security updates, but it's important to remember that software developers create these updates only after the bad guys have found ways to attack your system. The longer you wait to apply these patches and upgrades, the longer you leave your system vulnerable to hackers, spies and thieves.

Applications—especially programs that connect to the internet—also offer a way for attackers to access your system. For example, the makers of Java and Flash issue frequent updates to patch problems identified with those applications. If you use an application like these, keep it up-to-date. If you don't use an application, uninstall it. (Check with your IT team before making any changes!)

Leave It? Lock It.

Never leave your system logged in and unattended. Never: as in... not in your office at work, not on your desk at home, and not at your favorite local coffee shop. Never. When you walk out of eyesight of your device, lock it and/or log out. (On most Windows systems, just press Ctrl-Alt-Delete then Enter to lock it. Or, hold down the Windows key and press L.) Configure your system to automatically lock— and logout—after a few minutes if not in use.

SHARE THIS

Workstation security wrap-up

1. Use an active security suite
2. Update your software
3. Leave it? Lock it.
4. Don't share
5. Back up your data

Don't Share

Unless your IT team specifically tells you otherwise, don't share your system—with anyone. If you're the only one to use your system, you can keep it safe. Hand it to Alice in Accounting and she might insert a flash drive filled with malicious files. Loan your system to Bob in Marketing to use for a presentation at a conference and he might just present you with an infected file. When you share a file, share it from the company's shared file system—in the cloud or on your server. Don't use your personal Google Drive or Dropbox or OneDrive—and don't use anyone else's. Company-managed cloud services actively scan for problems, and your document server likely does, too. The same can't be said for Alice or Bob's DropBox or OneDrive accounts.

Keep things simple: don't share your system. Nobody borrows it—ever.

Back Up Your Data

Back up data you want to keep. You don't need to back up your operating system or applications— your IT team should be able replace and update those easily.

But your data isn't replaceable. That means your email, your documents, images, spreadsheets, presentations, audio and video files—all of it should be backed up.

Any file that matters to you should be backed up. This also includes cloud applications. It's true, just because you store data in the cloud does NOT mean it's automatically safe and protected. If your company is storing critical information in a SaaS application (like Salesforce), consider implementing a cloud-to-cloud backup solution.

With a backup, if your system does get infected—or when the hardware finally fails—your data is safe. You get another system, set it up, and then start work. A backup can save you the frustration of fighting with a malware infested system.

NETWORK SECURITY

Don't Connect to WiFi You Don't Own

A WiFi access point named "Free Hotel WiFi" or "Conference Center Guest" or "Coffee Shop Network" might not be provided by the hotel, convention center or cafe. Anyone can create a WiFi access point with that name. It may be very difficult to identify the difference—hence the name for this type of attack: The evil twin.

The evil twin access point looks legitimate, but isn't. When you connect your device to an evil twin, the attacker may access all the data that travels through the access point.

Never connect to an access point you don't control. Your WiFi network at work is likely safe: your tech team manages and monitors the WiFi environment. Elsewhere, tether your devices: create your own WiFi hotspot connection from your phone (here's how to do this from an Android or Apple phone). Or, connect directly to your mobile data provider's network—for example, with an iPad that connects to an LTE network. A villain can create an evil twin cell tower, but that's more difficult to do than to an evil twin WiFi access point.

Don't Connect to WiFi That Doesn't Require a Password

When you connect to a WiFi access point that doesn't require a passcode, the traffic between your device and the access point won't be encrypted. That means anything you do while connected to this WiFi network can be easily seen by others. Your usernames and passwords might be intercepted and viewed by a snoop scanning local WiFi traffic.

To guard against the local snoop, only connect to a WiFi access point that requires a passcode. The passcode encrypts the traffic between your device and the access point, and makes it more difficult for a local snoop to access your data. (Configure

SHARE THIS

Network security wrap-up

1. Don't connect to WiFi you don't own
2. Don't connect to WiFi without a password
3. Always use a firewall
4. Always use SSL

your home access point to use WPA2 encryption. Your organization also likely uses WPA2, but does so as part of an authentication system, so you might not see it.)

A virtual private network (VPN) also protects against a local snoop. A VPN connection encrypts traffic from your system to a system elsewhere—from your computer to a server at your company, for example. A local snoop would need to decrypt the data to access it.

Bottom line: Any WiFi you can use without a password is open to the public. Don't use them.

Always Use a Firewall

You use WiFi or Ethernet (the plugged-in version of the Internet) to get information into your system, but networks work in both directions. A hacker can use the Internet to access your computer or smartphone directly. A firewall protects your system from a remote attacker. Most organizations manage firewall settings in at least two places: one firewall that protects the organization's internet connection, and additional firewall on each individual Windows or Mac system. These settings are typically managed by your system administrator.

Enable the firewall on your home Mac or Windows system. Proper firewall settings may prevent unintentional file-sharing and access. If you use a WiFi router, check your manufacturer's instructions to access the administrative settings. Update the router's firmware, and verify that the router firewall is on. Most routers enable the firewall by default.

Firewalls make sure the only Internet traffic entering or leaving your network is the traffic you want. Don't use a network without a firewall.

Secure your SaaS data with Backupify

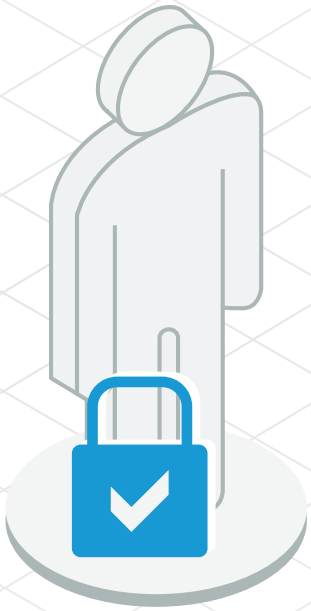
SCHEDULE A DEMO!

Always Use SSL in Your Web Browser

As you browse the web, your browser connects to servers all over the internet—and your data may travel many different routes. A traffic interceptor—a program or person that sits at an "intersection" on the information superhighway, randomly stopping traffic and examining what is inside—may access all of this data.

Encrypt your connection to protect your data in transit. That means that even if your information is stopped along the info superhighway by an interceptor, they won't be able to read it. It will be locked inside a secure container, safe from prying eyes. The basic form of web traffic encryption is called SSL, for Secure Sockets Layer (the name isn't important).

Many sites employ SSL by default. For example, if you type http://google.com to connect to Google, you'll notice that the link automatically redirects to https://google.com. The "https" indicates that traffic between your browser and Google's servers is encrypted with SSL. You'll also see a green lock (in most browsers) to indicate the connection is secure. Type https:// instead of http:// to connect to a site securely. (There's a plug-in that will do this for you automatically if you use Chrome or Firefox.) Unfortunately, not all sites support a secure connection.



PERSONAL & "SOCIAL" SECURITY

No matter how good the locks are on your front door, they don't matter if you invite a thief into your house. We've discussed the dangers of letting others borrow your smartphone or workstation, but those are just two examples of a so-called "social engineering attack" - which is a fancy term for hackers using con artist tricks to get around your computer security, rather than attacking your hardware or software directly.

None of the security practices we've outlined above will matter if you let a determined hacker sneak past them using social engineering. An informed and alert person remains the best defense against such attacks. To that end, consider the following practices.

Don't Talk to Strangers (Online)

Never respond to an email, text message, or phone call that requests any personal or private information. Such messages are easy to "spoof": to make appear as if they're from a legitimate source, but aren't.

If you receive such a request, contact the alleged source of the request directly over another channel. For example, if you receive an email from your bank requesting that you update your account information, call your bank at the phone number listed on your debit card. Don't call a phone number listed in the email: that might be a fraudulent number.

Similarly, never click a link "to update information" in an email. Instead, type the company's web address directly into your browser and login to your account. A link might take you to a site that appears authentic, but isn't. Type links, don't trust links.

SHARE THIS

Social engineering wrap-up

1. Don't talk to strangers online
2. Only give out data on phone calls that you've started
3. Watch your back
4. Everybody you just met is a stranger, no matter what they "know"

Only Give Out Data In Phone Calls That You've Started

Never provide account information over the phone—unless you placed the call. This especially applies to tech support services that will "call you back". If you're trying to resolve a tech issue, always initiate the call; never disclose information to an incoming caller. As above, don't write down a number provided by the caller: look up the correct main support number, and then call the person.

Watch Your Back

Always be aware of your surroundings—including people and objects outside your field of view. There may be people behind or above you. Look for them. A thief might follow you past a door you've unlocked. A hacker might be snooping over your shoulder as you type your password or PIN.

Even better, never work with sensitive information on your laptop in a public setting. If you must do so, sit like a lawman in a classic western: with your back to the wall.

Everybody You Just Met Is A Stranger, No Matter What They "Know"

Be aware of false friends online and in person. A lot of information about you might be available online: where you went to school, where you worked, your hobbies, your interests, family members, and networks of friends. Even places you frequent might be online if you "check-in" at locations you visit.

All of that information can be used to establish false familiarity. "Oh, I went Sunnydale High, too.

Did you happen to know Buffy Summers?" Such a phrase can reduce your reluctance to talk to a stranger. You're simply reminiscing with a friend, right? Maybe not. Be careful not to disclose sensitive information in such a setting. This new "friend" might be a well-prepared hacker looking to con you out of crucial information.

backupify

a datto company

- **Unmatched cloud expertise** from the global leaders in SaaS protection
- **The cost-effective** choice for the Enterprise, offering a reliable, fast, automated, and scalable solution
- **Truly secure**, independent backup that is SOC 2 Type II & HIPAA compliant
- **Quickly recover data** from ransomware, accidental deletion, or human error with Backupify's infinite retention and unlimited storage

Find out why over 3 million users around the globe trust Backupify to protect their Office 365 and G Suite data.

Start your 15-day free trial at Backupify.com.

Conclusion

Computer security can be complicated and intimidating for the average user. It's tempting to simply give your users a list of things to not do and demand they follow it, no matter how annoying or confusing those instructions might be.

If you take the time to explain why your company uses certain types of security software, or requires specific security procedures, your users are much more likely to take these lessons to heart. User error is one of the leading causes of data loss but, with a little education, you can reduce the risks of your users damaging or disclosing your business data.

(But we'd still recommend a good backup plan.)

SECURITY 101 CHECKLIST

PASSWORD SECURITY

- ☐ Never share your password with anyone, ever
- ☐ Use a passphrase (a short sentence that's easy to remember) instead of a password. Combine your passphrase with two-factor authentication

EMAIL SECURITY

- ☐ Never respond to an email from strangers
- ☐ Don't open any attachments that you haven't scanned first
- ☐ Don't open any links you haven't checked (hint, hover over the link to ensure it's really going where it's supposed to go)
- ☐ Always back up your email

WEB BROWSER SECURITY

- ☐ Only install from safe sources (hint, the vendor's download site or your browser's add-in store)
- ☐ Look for the lock and ensure you see the icon before entering your personal information into a website Save and sync selectively when asked "Would you like to store this password?" The best answer is NO. If you log in then you should also log out - always
- ☐ Clear and back up everything

SMARTPHONE SECURITY

- ☐ Always use a lock screen - every smartphone and tablet have one. Use it.
- ☐ Nobody should ever borrow your smartphone
- ☐ Don't respond to a text from a stranger
- ☐ Don't answer calls from strange phone numbers - it's better to screen these calls. Let voicemail handle it. Back up everything

WORKSTATION SECURITY

- ☐ Use an active security suite, aka an antivirus program to protect your system from viruses such as malware, spyware, and network attacks
- ☐ Update your software - keep your operating system, security suite, and programs up-to-date Leave it? Lock it. Don't leave your system logged in and unattended
- ☐ Don't share your system with anyone unless specifically told by your IT team
- ☐ Back up your data

NETWORK SECURITY

- ☐ Never connect to Wi-Fi that you don't own Don't connect to Wi-Fi without a password Always use a firewall
- ☐ Always use SSL in your web browser

SOCIAL ENGINEERING

- ☐ Don't talk to strangers online
- ☐ Only give out data on the phone calls that you started
- ☐ Watch your back - literally. Be aware of your surroundings when in public and logged on to your computer
- ☐ Everybody you just met is a stranger, no matter what they claim to "know" - the best advice for online and in person as well.