



Keeping Your Phone and Accounts Safe on the Road

Guard Your Accounts Simple habits for public Wi-Fi charging stations and lost phones

————— An Extended Guide · No. 1607 —————

Tech Made Simple. Service Made Personal.

Bill Davis — Bill's Home Tech

(330) 200-8042 · bill@billshometech.com · Atwater, Ohio

Book a visit — billshometech.com/book

What's Inside

Everything in this guide, with page numbers. Skip to whichever chapter answers your question right now.

1. The Whole Idea in One Glance	5
2. Why Travel Is When Trouble Finds People	5
3. Lock the Phone Itself	6
4. Why Face ID and Fingerprints Help	6
5. What Public Wi-Fi Really Is	6
6. What Is Safe and What Can Wait	7
7. What a VPN Does, in Plain Words	7
8. Picking a VPN Without Overthinking It	8
9. Turning the VPN On When It Counts	8
10. Why Public USB Ports Are a Hidden Risk	9
11. The Three Safe Ways to Charge	9
12. The Power Bank, a Traveler's Best Friend	9
13. The Little Adapter That Blocks Data	10
14. The Trick of the Fake Wi-Fi Network	10
15. How to Join a Public Network the Right Way	11
16. The Eyes Over Your Shoulder	11
17. Passwords That Hold Up	12
18. Letting a Password Manager Do the Remembering	12
19. Two-Factor Authentication, the Second Lock	13
20. Turning On Two-Step Login Before You Go	13
21. Backup Codes, Your Spare Key	14

22. Back Up the Phone Before You Leave	14
23. Switch On Find My Before You Travel	14
24. Carry Less, Risk Less	15
25. Updates Are Quiet Protection	15
26. Minding What Apps Can See	16
27. The Scam Text and the Fake Email	16
28. Paying With Your Phone Is Safer Than You Think	17
29. A SIM PIN, the Lock Most People Miss	17
30. Closing Doors You Are Not Using	17
31. Safety Inside the Hotel Room	18
32. Why to Avoid Shared Computers	18
33. If an Account Is Broken Into While You Travel	19
34. If You Cannot Get Into Your Own Account	19
35. Keep a Trusted Person in the Loop	20
36. Protecting Banking and Wallet Apps	20
37. Set Up the Phone to Help in an Emergency	20
38. A Simple Daily Habit on the Road	21
39. The Questions Travelers Ask Me Most	21
40. Enough Caution, Not Too Much	22
41. Your Pre-Trip Safety Checklist	22
42. When It Is Worth Calling Me	22
Everyday Cheat Sheet	23
A Picture to Follow Along	24

A Second Look 25

A Note From Bill 25

Your Visit — and My Promise 26

THE 60-SECOND VERSION

1. The Whole Idea in One Glance

If you remember only this page, you will still be far safer than most travelers.

Keeping safe on the road is not about fancy gadgets or being a computer expert. It is about a few small habits that take seconds and head off almost every problem. Do these and you can relax and enjoy your trip.

- Lock your phone with a PIN or your face, and keep it with you
- On public Wi-Fi, avoid banking unless you are using a VPN
- Charge from your own plug or power bank, not a public USB port
- Turn on the free two-step login for email and banking before you leave
- Back up your phone before the trip so nothing is truly lost

GOOD TO KNOW

Thieves and scammers go after the easy targets. A locked phone, a backed-up account, and a bit of care on open Wi-Fi make you a hard target, and most trouble simply passes you by.

WHY IT MATTERS

2. Why Travel Is When Trouble Finds People

At home you are on your own Wi-Fi, you charge from your own wall, and your routine is familiar. On a trip, every one of those comforts changes. You join networks you have never seen, you plug into strange outlets, and you are tired, distracted, and carrying everything you own in one bag.

That is exactly the mix that lets small mistakes happen. The good news is that the fixes are small too. A few minutes of setup before you leave, and a few easy habits while you are out, cover the great majority of the risk.

WATCH OUT

You do not need to do everything in this guide to be much safer. Even the first three or four habits put you ahead of nearly everyone around you at the airport.

FIRST THINGS FIRST

3. Lock the Phone Itself

Your phone is the key to everything else: your email, your photos, your bank app, your messages. If a stranger can pick it up and swipe in, none of your other precautions matter. So the first habit is the simplest: never leave your phone unlocked.

- Set a passcode of at least six digits, not four
- Turn on Face ID or a fingerprint so unlocking is quick for you
- Set the screen to lock itself after a short idle time
- Never leave the phone face-up and unattended on a cafe table

WATCH OUT

Avoid an obvious passcode like 1234 or your birth year. A thief who watched you type it, or who knows your birthday, can be into your phone in seconds.

FACE OR FINGER

4. Why Face ID and Fingerprints Help

Unlocking with your face or a fingerprint is not just faster, it is safer. When you use it, you type your passcode far less often, which means fewer chances for someone nearby to watch you enter it. The code stays in your head where it belongs.

Both Apple and Android phones store your face or fingerprint only on the phone itself, locked away where apps and companies cannot reach it. It is not uploaded anywhere. So turning it on costs you nothing in privacy and saves you from tapping in a code at every glance.

TIP

If arthritis or dry skin makes a fingerprint reader fussy, face unlock is often easier. Try both and keep whichever one works smoothly for your hands.

THE OPEN AIR

5. What Public Wi-Fi Really Is

Public Wi-Fi is any network you did not set up yourself: the airport, the hotel, the coffee shop, the cruise terminal. It is wonderfully handy and perfectly fine for plenty of things. The catch is that you are sharing that network with every stranger in range, and you cannot know who set it up.

Think of it like talking in a crowded waiting room. Chatting about the weather is fine. Reading your bank balance aloud is not. The network is the room; some things are simply better kept private.

GOOD TO KNOW

Most websites and apps today scramble their traffic on their own, which helps a great deal. But on an unknown network, the safest habit is still to save your most sensitive tasks for later or use a VPN.

SAFE ON OPEN WI-FI

6. What Is Safe and What Can Wait

You do not need to avoid public Wi-Fi altogether. You just need to know which tasks are fine on it and which are worth holding until you are on a network you trust or using a VPN.

- Fine anywhere: reading news, checking maps, watching videos, browsing
- Fine: email and messaging, which scramble themselves on their own
- Better to wait or use a VPN: logging into your bank or moving money
- Better to wait: entering a credit card to buy something

TIP

If you must check your bank balance on the road, use your phone's own cell data instead of the hotel Wi-Fi, or switch on a VPN first. Cell data is private to you in a way open Wi-Fi is not.

VPN BASICS

7. What a VPN Does, in Plain Words

VPN stands for virtual private network, but forget the name. Picture it as a sealed tunnel for your internet. Without it, what you do on open Wi-Fi travels through the open room where others could listen. With a VPN on, everything goes through a private tunnel that nobody in that room can read.

You turn it on with a single switch in an app, and then you use your phone exactly as always. It runs quietly in the background. When you are back on a network you trust, you can switch it off.

GOOD TO KNOW

A VPN protects what you do on the network. It does not make you anonymous or stop you from being fooled by a scam. It is one useful tool among several, not a magic shield.

CHOOSING A VPN

8. Picking a VPN Without Overthinking It

There are many VPN apps, and the honest truth is that for an occasional traveler, most of the well-known paid ones are fine. Stick to a reputable, paid service rather than a free one, because a free VPN has to make money somehow, often by selling the very data you were trying to protect.

- Choose a well-known paid service with a clear, simple app
- Install it and sign in at home, before your trip, where you can test it
- Avoid free VPNs that may log and sell your activity
- One subscription usually covers your phone, tablet, and laptop

TIP

Prices change, so confirm the current cost before you subscribe. As a rough guide, a year of a good VPN costs in the range of a few nice dinners out, often less per month than a single coffee.

USING A VPN

9. Turning the VPN On When It Counts

Once the app is installed, using it is a single tap. The habit to build is simple: before you do anything sensitive on a network that is not yours, flip the VPN on first.

- 1 Connect to the airport or hotel Wi-Fi as usual
- 2 Open your VPN app
- 3 Tap the big Connect button and wait for it to say connected
- 4 Now do your banking or shopping as normal
- 5 Switch the VPN off once you are back on trusted Wi-Fi or done

GOOD TO KNOW

Some VPN apps can turn themselves on automatically whenever you join an unknown network. If yours offers that, switch it on and you will never have to remember.

THE CHARGING TRAP

10. Why Public USB Ports Are a Hidden Risk

You have seen them everywhere: a USB slot built into an airport seat, a hotel lamp, or a rental car. It feels like a gift when your battery is low. But a USB port can carry data as well as power, and the FBI and the FCC have both warned that a tampered port or a planted cable could, in theory, push harmful software onto your phone or pull data off it. The nickname for this is juice jacking.

The simple, foolproof fix is to never put your phone's data wire into a public USB slot. Bring your own way to charge instead, and the whole worry disappears.

WATCH OUT

Be especially wary of a charging cable someone left plugged in, or a free cable handed out as a giveaway. A rigged cable looks exactly like a normal one. Use only your own cables and chargers.

CHARGE SAFELY

11. The Three Safe Ways to Charge

You never have to use a public USB port, because there are three easy ways to charge that carry no risk at all. Pack for these and you can skip every suspicious slot.

- Use your own charging block in a regular wall outlet, which carries power only
- Carry a power bank, a pocket battery you charge at home and top up from
- If you must use a public USB port, plug in through a USB data blocker
- Charge overnight in your own hotel room from your own wall plug

TIP

A wall outlet with your own plug is always safe, because a wall socket only delivers power and cannot carry data. The USB slot is the only part to be cautious about.

POWER BANKS

12. The Power Bank, a Traveler's Best Friend

A power bank is a small battery, about the size of a deck of cards or a candy bar, that you charge up at home and carry in your bag. When your phone runs low, you plug it into the power bank instead of hunting for an outlet. It is the single easiest way to never need a public charger.

One charge of a decent power bank will refill a phone a couple of times over. You charge the bank itself overnight from your own wall plug, and it is ready for the next day out.

GOOD TO KNOW

Power banks must fly in your carry-on bag, never in a checked bag, because of airline battery rules. Keep yours in the bag that stays with you on the plane.

DATA BLOCKERS

13. The Little Adapter That Blocks Data

If you really want the convenience of public USB ports without the risk, a USB data blocker solves it. It is a tiny adapter, cheaper than a sandwich, that you put between your cable and the public port. It lets power through but physically blocks the data lines, so nothing can be sent to or taken from your phone.

GOOD TO KNOW

A data blocker is sometimes called a USB condom, an awkward name for a handy little thing. Keep one on your keychain or in your travel pouch and a public charger becomes harmless.

FAKE NETWORKS

14. The Trick of the Fake Wi-Fi Network

One scam worth knowing about is the fake network, sometimes called an evil twin. A scammer sets up their own Wi-Fi and names it something believable, like Airport Free WiFi or Hotel Guest, hoping you will join it by mistake. Once you do, they sit between you and the internet.

The defense is simple. Before you join any network, ask a staff member for the exact name of the real one. Do not just pick the first familiar-looking name in the list.

WATCH OUT

Be suspicious of any network that asks for your email password, your credit card, or a software download just to get online. A real public network does not need those things.

JOINING SAFELY

15. How to Join a Public Network the Right Way

Joining a public network safely takes just a few extra seconds of care. The habit is to confirm the real name first and to turn off the setting that makes your phone leap onto networks on its own.

- 1 Ask a staff member, or check posted signs, for the exact network name
- 2 Choose that exact name from your phone's Wi-Fi list, matching it letter for letter
- 3 If you are doing anything sensitive, turn your VPN on
- 4 When you leave, tell your phone to forget the network so it will not auto-join later

GOOD TO KNOW

Turn off your phone's setting to automatically join open networks. Otherwise it may silently connect to a fake network as you walk past, without you ever choosing it.

SHOULDER SURFING

16. The Eyes Over Your Shoulder

Not every threat is high-tech. One of the oldest tricks is simply watching you type. In a crowded gate area or a train, someone nearby can read your screen or watch your fingers as you enter a passcode or a password. This is called shoulder surfing, and it is more common than people think.

- Shield the screen with your hand when typing a passcode in a crowd
- Use face or fingerprint unlock so you type the code less often
- Turn your phone away from the person seated beside you on a plane
- Be aware of mirrors and reflective windows behind you

TIP

A privacy screen protector, a thin film over your screen, makes the display look dark to anyone not sitting directly in front of it. It is a cheap, quiet way to keep nosy neighbors out of your business.

STRONG PASSWORDS

17. Passwords That Hold Up

A strong password is your front door lock for every account. The old advice to use a short jumble of symbols is out of date. A longer phrase is both stronger and far easier to remember. Length is what matters most.

- Use a phrase of several words, like PurpleBarnKent1952, rather than a short jumble
- Make it at least a dozen characters long
- Never reuse the same password on your email and your bank
- Do not use your name, your pet, or your birthday, which others can guess

GOOD TO KNOW

Your email password is the most important one of all, because anyone who gets into your email can reset the password on everything else. Make that one especially strong and unique.

PASSWORD MANAGERS

18. Letting a Password Manager Do the Remembering

Nobody can remember a different strong password for dozens of accounts, and you should not try. A password manager is a secure app that remembers them all for you, locked behind one master password or your face. Both Apple and Google build one into the phone for free.

When you travel, this means you can use a long, unique password on every account without the worry of forgetting them. You unlock the manager with your face, and it fills in the rest.

TIP

If a password manager feels like a step too far, that is fine. Keep a small notebook of your passwords at home, not in your travel bag, and bring only the few you truly need.

TWO-STEP LOGIN

19. Two-Factor Authentication, the Second Lock

Two-factor authentication, also called two-step verification, is the single best thing you can turn on. It means that even if someone learns your password, they still cannot get in without a second code that only you receive. It is like needing both a key and a fingerprint for the same door.

That second step is usually a short code texted to your phone, or a tap in an app, or a prompt on a device you own. Turn it on for your email, your bank, and your main accounts before you travel.

GOOD TO KNOW

This is why keeping your phone locked and with you matters so much: your phone is often the second key. If it is safe, your accounts stay safe even if a password leaks.

SETTING IT UP

20. Turning On Two-Step Login Before You Go

Setting up two-step login takes a few minutes per account and you only do it once. Do it at home, well before the trip, so you can fix any snags calmly rather than at a boarding gate.

- 1 Open the settings or security page of your email or bank account
- 2 Look for Two-Factor Authentication or Two-Step Verification and turn it on
- 3 Choose how to get your code: a text, an app, or a security key
- 4 Enter a test code to confirm it works
- 5 Save your backup codes somewhere safe at home

WATCH OUT

If you are traveling overseas, a text code may not reach a phone without international service. Set up an authenticator app as a backup, or save the printed backup codes, so you are never locked out abroad.

BACKUP CODES

21. Backup Codes, Your Spare Key

When you turn on two-step login, most accounts offer you a list of one-time backup codes. These are a spare key for the times your phone cannot receive the normal code, such as abroad with no signal, or if the phone is lost. Each code works once.

TIP

Print your backup codes and tuck them in your wallet or a separate pouch, apart from your phone. If your phone goes missing, those codes let you get back into your email from any other device.

BACK UP FIRST

22. Back Up the Phone Before You Leave

A backup is a complete copy of what is on your phone, kept safely in the cloud. If your phone is lost, stolen, or dropped in a pool, a backup means your photos, contacts, and messages are not gone. You simply restore them to a new phone and carry on. This is the single most reassuring thing you can do before a trip.

- iPhone: turn on iCloud Backup in Settings, then let it finish on Wi-Fi
- Android: turn on backup to your Google Account in Settings
- Make sure your photos are set to upload to iCloud or Google Photos
- Confirm the backup finished before you walk out the door

GOOD TO KNOW

A backup turns a lost phone from a disaster into an expense. The phone can be replaced; the photos of your grandchildren cannot, unless they are backed up.

FIND MY PHONE

23. Switch On Find My Before You Travel

Every modern phone can be located, locked, and even erased from afar, but only if you switch on that feature ahead of time. On an iPhone it is called Find My; on Android it is Find Hub. Turn it on at home and you will have a calm plan ready if the phone ever goes missing.

There is a companion guide devoted entirely to what to do when a phone is lost or stolen away from home. The one thing to do in advance is simply to make sure this feature is

turned on.

TIP

Take a moment before the trip to open Find My or Find Hub and confirm your phone shows up on the map. If it does, the safety net is in place.

LESS TO CARRY

24. Carry Less, Risk Less

The simplest security of all is to not carry what you do not need. Every extra card, device, or sensitive app in your bag is one more thing to lose. Pare down before you pack and there is less to protect and less to replace.

- Leave cards you will not use on the trip at home
- Remove apps you do not need, especially any you rarely open
- Take a photo of the front of the cards you do carry, kept in a locked notes app
- Bring one main credit card and one backup, not your whole wallet

GOOD TO KNOW

Keeping a photo of your cards and passport in a secure, locked note on your phone means that if a wallet is lost, you have the numbers to cancel cards quickly.

APP UPDATES

25. Updates Are Quiet Protection

Those update reminders you keep putting off are not just new features. Many of them quietly patch security holes that bad actors look for. A phone that is up to date has fewer open doors, which matters most when you are out on networks you do not control.

TIP

Update your phone and your apps at home, on your own Wi-Fi, the day before you leave. Then you start the trip current and you are not downloading large updates on a slow hotel connection.

LOCATION SETTINGS

26. Minding What Apps Can See

Many apps ask to know your location, read your contacts, or use your camera. For plenty of them, there is no good reason. Trimming these permissions is a gentle way to keep your travel private and your battery lasting longer.

- In Settings, review which apps can see your location and switch off the ones that do not need it
- Set location-hungry apps to 'While Using' rather than 'Always'
- Turn off Bluetooth and Wi-Fi scanning when you are not using them
- Be thoughtful about posting your location on social media while away

WATCH OUT

Posting photos that show you are far from home tells the world your house is empty. Many travelers wait until they are home to share the vacation album.

PHISHING

27. The Scam Text and the Fake Email

While you travel, you may get texts or emails that look official: a delivery problem, a bank alert, a message about your lost phone, a fare change. Many are fakes designed to make you panic and tap a link. The link leads to a page that steals your password. This is called phishing, and travel is a favorite time for it because you are busy and expecting messages.

- Never tap a link in an unexpected text or email asking you to log in
- Instead, open the app or type the website address yourself
- Be wary of anything urgent that pressures you to act immediately
- Your bank and Apple will never text you asking for your password

TIP

When in doubt, stop and call the company using the number on the back of your card or your statement, not any number in the message. A real problem will still be there after you check.

TAP TO PAY

28. Paying With Your Phone Is Safer Than You Think

It may feel safer to hand over a plastic card, but paying with Apple Pay or Google Wallet by tapping your phone is actually more secure. Your real card number is never shared with the store. The phone sends a one-time code instead, so there is nothing for a crooked card reader to steal.

Because each payment needs your face or fingerprint to approve, a thief with your phone cannot simply tap and buy. It is one of the few cases where the newer way is plainly the safer way.

GOOD TO KNOW

Tap-to-pay also sidesteps skimmers, the hidden devices criminals attach to card slots at gas pumps and ATMs. If you can tap, you avoid the slot entirely.

LOCK THE SIM

29. A SIM PIN, the Lock Most People Miss

The small SIM card inside your phone is what connects you to your carrier. If a thief pops it into another phone, they can receive your calls and texts, including some security codes. A SIM PIN is a short code that locks the SIM so it is useless in anyone else's phone.

WATCH OUT

You can turn on a SIM PIN in your phone's settings. Set it at home and keep the code somewhere safe, because you will be asked for it whenever the phone restarts. It is an easy extra lock most travelers never think of.

BLUETOOTH AND AIRDROP

30. Closing Doors You Are Not Using

Features that let your phone talk to nearby devices, like Bluetooth and the file-sharing tools, are handy at home but are open doors in a crowd. When you are not using them, a quick switch-off keeps strangers from even trying to connect or send you unwanted files.

- Turn Bluetooth off when you are not using earbuds or a car
- Set iPhone AirDrop to receive from Contacts Only, not Everyone
- Ignore and decline any file or photo a stranger tries to send you

- Turn off the personal hotspot when you are not sharing your connection

GOOD TO KNOW

On an iPhone, leaving AirDrop open to Everyone in a crowded airport can bring unwanted and sometimes alarming images from pranksters. Contacts Only stops that cold.

HOTEL ROOM

31. Safety Inside the Hotel Room

A hotel room is not as private as your home. Housekeeping, maintenance, and others have keys. A few simple habits keep your devices and your accounts safe while you are out seeing the sights.

- Use the in-room safe for your passport, spare cards, and any device you leave behind
- Lock your laptop and tablet, not just your phone
- Do not leave written passwords lying on the desk
- Log out of any shared lobby computer completely when you finish

WATCH OUT

Avoid typing passwords on a hotel lobby or business-center computer at all. You cannot know what is installed on it. Use your own phone or laptop for anything private.

PUBLIC COMPUTERS

32. Why to Avoid Shared Computers

A computer in a hotel lobby, a library, or an internet cafe is used by strangers all day long. You have no idea whether it secretly records what is typed on it. For printing a boarding pass it is fine; for logging into your email or bank, it is a bad idea.

TIP

If you ever must sign in on a shared computer, change that password from your own phone the moment you can, and always log out fully rather than just closing the window.

IF IT HAPPENS

33. If an Account Is Broken Into While You Travel

Suppose you get a sign-in alert you did not make, or you suddenly cannot log in. Do not panic. A calm, quick response usually shuts the problem down before any harm is done. The order of operations matters: lock down your email first, because it controls everything else.

- 1 From a device you trust, change the password on your email first
- 2 Then change the password on the account that was broken into
- 3 Turn on two-step login if it was not already on
- 4 Sign out all other devices from the account's security settings
- 5 Call your bank if any money account is involved

GOOD TO KNOW

Most accounts have a 'sign out of all devices' button in their security settings. One tap kicks out anyone who got in, and your new password keeps them out.

FROZEN OUT

34. If You Cannot Get Into Your Own Account

Sometimes the trouble is that you are locked out: a forgotten password, a phone that will not receive the code, or an account that got changed. This is where the preparation you did at home pays off. Your backup codes and a second device are your way back in.

- Use the printed backup codes you saved before the trip
- Try the account's 'forgot password' option from a trusted device
- Use a second device, like a tablet, that is already signed in
- Call the company's official support line, found on their website, for help

TIP

This is the reason to set up two-step login and save backup codes before you leave, not during a crisis abroad. A few minutes at home saves hours of worry on the road.

TELL THE FAMILY

35. Keep a Trusted Person in the Loop

You do not have to handle a problem alone. Before you go, let a trusted family member know your travel dates and how to reach you. If an account is compromised or a phone is lost, a second pair of hands at home can help you from a computer you both trust.

GOOD TO KNOW

Share your itinerary with someone you trust, not the whole internet. A family member knowing where you are is a safety net; a public post is an invitation to trouble at an empty house.

BANKING APPS

36. Protecting Banking and Wallet Apps

The apps that touch your money deserve the most care. The good news is they are built to be well defended, and a couple of settings make them tougher still. Treat them as the crown jewels of your phone.

- Turn on the app's own face or fingerprint lock, so it needs a second unlock
- Set up alerts so your bank texts you on any large charge
- Keep the bank's real phone number saved in your contacts
- Never do banking on a public computer, only on your own locked phone

TIP

Many bank apps let you require a separate face or fingerprint scan to open them, even after your phone is unlocked. Switch that on for a second line of defense.

EMERGENCY INFO

37. Set Up the Phone to Help in an Emergency

Your phone can carry emergency information that shows even on a locked screen, so a first responder or a good Samaritan can help you and reach your family. This is quiet peace of mind for any trip, and it takes only a few minutes to set up.

TIP

On an iPhone, fill in the Medical ID in the Health app and add emergency contacts. On Android, set up the Emergency information in Settings. Both show on the lock screen without unlocking the phone.

A CALM ROUTINE

38. A Simple Daily Habit on the Road

Security on a trip is not a one-time chore; it is a light daily habit, like checking you have your keys. None of it takes long, and once it is a rhythm you barely notice it.

- Morning: top up your power bank and phone from your own wall plug
- Out and about: keep the phone locked and in a front pocket or zipped bag
- On open Wi-Fi: flip the VPN on before anything sensitive
- Evening: glance at your bank alerts and that your phone shows on Find My

GOOD TO KNOW

The whole routine adds up to a couple of minutes a day. For that small effort, you trade away most of the worry and get to simply enjoy your trip.

COMMON WORRIES

39. The Questions Travelers Ask Me Most

A handful of worries come up again and again, and the answers are reassuring.

- Is airport Wi-Fi safe? Fine for browsing; use a VPN for banking
- Will charging my phone from the wall hurt it? No, a wall plug is always safe
- Do I really need a VPN? Helpful but optional; cell data is private too
- Can someone steal my card by tapping my phone? No, tap-to-pay shares no real number

GOOD TO KNOW

Most travel trouble comes from a lost or unlocked phone, not from clever hackers. Lock the phone, back it up, and you have handled the biggest risk by far.

DON'T OVERDO IT

40. Enough Caution, Not Too Much

It is possible to worry too much and tie yourself in knots. The goal is a handful of good habits, not fear. Almost everyone travels with a phone and comes home with no trouble at all. You are reading this so you will be among them.

TIP

Pick the habits that feel easy and do those first: lock the phone, back it up, charge from your own plug, turn on two-step login. Add the rest as you grow comfortable.

BEFORE YOU GO

41. Your Pre-Trip Safety Checklist

Run through this list in a calm hour before you leave, and you are set for a safe trip.

- Phone locked with a six-digit code and face or fingerprint unlock
- Phone backed up and photos uploading to the cloud
- Two-step login turned on for email and bank, backup codes printed
- A VPN installed and tested, a power bank charged
- Find My or Find Hub confirmed working
- Updates installed, unused apps and spare cards left at home

GOOD TO KNOW

Do this the day before, not in the car to the airport. A relaxed half hour at the kitchen table is all it takes, and you leave with nothing nagging at you.

WHEN TO CALL

42. When It Is Worth Calling Me

Most of this you can set up yourself in an afternoon. But if the settings feel like a maze, if you are not sure your backup really worked, or if you would simply rather have someone sit beside you and walk through it, that is exactly what I am here for. I can get your phone and your accounts trip-ready in one visit.

Bill's Home Tech serves Portage County with in-home help, and I bring over thirty years of experience to making this plain and painless. The first in-home visit is a flat ninety-nine dollars, remote screen-share help is forty-nine, and every visit includes a thirty-day follow-up.

TIP

Call Bill at (330) 200-8042, or ask Sophie, our phone and chat helper, to get you started. One visit before your trip and you can travel knowing your phone and accounts are locked down tight.

CHEAT SHEET

Everyday Cheat Sheet

Keep this page handy for your trip. It is the short answer to the questions travelers ask most about staying safe on the road.

- Lock your phone with a six-digit code plus face or fingerprint
- On public Wi-Fi, browse freely but turn on a VPN before banking
- Charge from your own wall plug or power bank, never a public USB port
- Carry a USB data blocker if you ever must use a public port
- Turn on two-step login for email and bank; print the backup codes
- Confirm the real Wi-Fi name with staff before you join
- Shield your screen when typing a passcode in a crowd
- Back up your phone and turn on Find My before you leave home
- If an account is breached: change your email password first, then sign out all devices
- Get help: call Bill at (330) 200-8042

AT A GLANCE

A Picture to Follow Along

Three Safe Ways to Charge

Skip the public USB port and you skip the risk.

Wall Plug

Your own charger block
Into a regular outlet
Power only, no data

Power Bank

Pocket battery you carry
Charged at home
Flies in carry-on only

Data Blocker

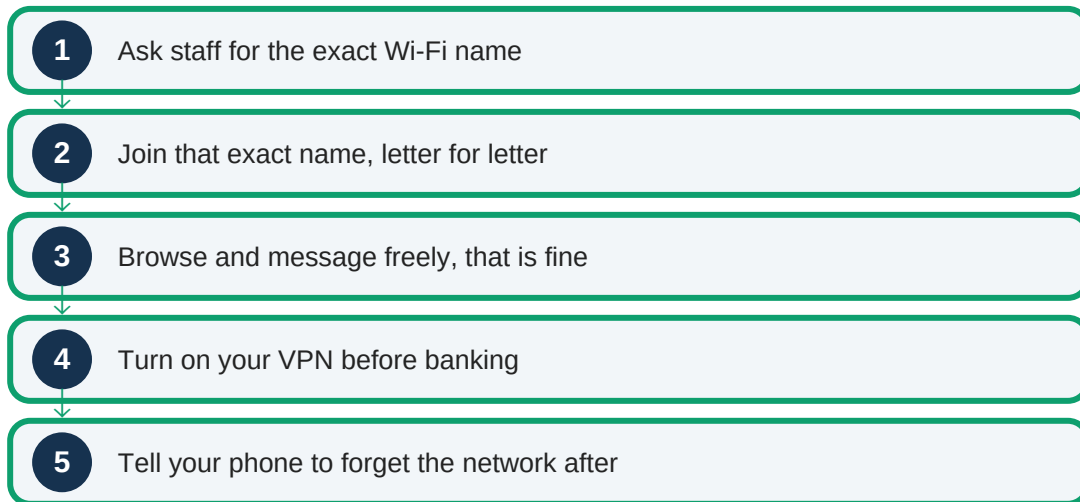
Tiny adapter on cable
Lets power through
Blocks the data lines

AT A GLANCE

A Second Look

Using Public Wi-Fi Safely

A few seconds of care covers almost every risk.



BEFORE YOU GO

A Note From Bill

A quick note from Bill. I write these guides to make home tech a little less frustrating, and I do my best to keep every step accurate and up to date. Still, every home, device, and setup is a bit different, so I can't promise a guide will match yours exactly or fix your particular problem. These guides are for general information only — they're not professional, legal, or financial advice, and they don't replace your device's own manual or the manufacturer's instructions. Please go slow, use your own good judgment, and use everything here at your own risk. If a step involves electrical wiring, a gas appliance, a water heater, plumbing, or climbing a ladder — or if anything just doesn't feel safe — please stop and call a licensed professional (or give me a call at 330-200-8042). Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results.



HOW I CAN HELP

Your Visit — and My Promise

In-home visit — \$99 flat for your first visit. No contracts and no surprise charges, and a 30-day follow-up is included.

Remote Support — \$49 for a screen-share session. I only connect with your permission, you watch the whole time, and you can end anytime. If I can't fix it over the screen-share, I refund the \$49 — and if it turns out you need me in person, that \$49 goes toward your visit. It's included free for Support Plan members (\$39/mo).

GOOD TO KNOW

My promise — If you're not 100% satisfied with your visit, I'll come back at no charge, or refund the full \$99. No questions, no awkwardness. That's how I'd want to be treated.

Call or text **(330) 200-8042** · Book a visit: billshometech.com/book · bill@billshometech.com

This free guide is for general information only — not professional advice, and no substitute for your device's own manual. Any prices or outside products mentioned can change; please confirm current details before you buy. Please use your own good judgment and follow it at your own risk — for anything involving electricity, gas, water, or heights, stop and call a licensed professional. Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results. © 2026 Bill's Home Tech, LLC.