Borderless Digital Shield™

Quick Start Guide

CREATE YOUR OWN *PRIVATE BUSINESS SPACE* ONLINE IN ABOUT 10 MINUTES.

FOR SMALL ONLINE BUSINESSES, FREELANCERS, AND SIDE HUSTLERS WHO RUN EVERYTHING FROM A LAPTOP, A PHONE, AND THE NEAREST WI-FI NETWORK.

Presented by Cybersolutionz

WWW.DKSOLUTIONZ.COM
DAVID@DKSOLUTIONZ.COM

Borderless Digital Shield™
- Toolkit Quick Start Card

Borderless Digital Shield™ is a practical toolkit for small online businesses, freelancers, and side hustlers who are running a whole business on a laptop, a phone, and whatever Wi-Fi is available. The 5-Step Work-Anywhere Checklist includes 3 steps and 2 rules that turn the public internet into your Private Business Space in about 10 minutes. The two rules and bonus cards included build on the checklist and show you how to protect your money, storefront, and platforms with the same simple rules.

Who this is for

You run a small online business, freelance practice, or side hustle. Your whole business probably lives on: One laptop • One phone • A few "good enough" passwords • Whatever Wi-Fi is available • This toolkit is here to make you a hard target without turning you into an IT department.

What's inside

Checklist plus cards that focus on the places small businesses actually get hurt:

• Work-Anywhere Wi-Fi Shield – don't get burned by public Wi-Fi

• Payables Safety Card – stop wires and invoices going to scammers

• Ransomware Shield – so one weak password doesn't kill your business

• IG Shield – protect your storefront handle

• Creator Shield – protect the trust your audience has in your links

• Platform Shield – protect income flowing through apps you don't control

Your Private Business Space

The Big Idea behind Borderless Digital Shield™ is simple - You create a Private Business Space online where:

• Your VPN is ON when you're doing money or client work

• You use one business-only browser/profile

• A password manager holds your long, ugly, unique passwords

Outside of that space, you scroll. Inside that space, you run your business.

How to use the cards

1. Start with the card that matches your biggest fear (Wi-Fi, money, IG, etc.).

2. Pick one change you can make in the next 24 hours.

3. Mark your progress on the Scorecard.

4. Revisit the cards whenever your business or tools change.

Why this matters

If your business fits in a backpack, your "office" is whatever Wi-Fi you're on right now. Airports, hotels, and coffee shops are convenient—but they're also places where attackers quietly watch logins on fake or insecure networks.

Borderless Digital Shield™

- 5 Step Work-anywhere checklist

Quick Start Checklist

- ☐ Move 1 – VPN + Kill Switch
- ☐ Move 2 – Passkeys / Password Manager
- ☐ Move 3 – Threat Protection
- ☐ Rule 1 – Use non-admin accounts for daily work.
- ☐ Rule 2 – Backups - Onsite and offsite storage.

+ Troubleshooting & Tips

The 3 Moves

1) VPN + Kill Switch

- Install on phone, laptop, and desktop.
- Enable **Kill Switch** to keep traffic encrypted if Wi-Fi drops.
- Auto-connect on untrusted Wi-Fi/open networks (cafés, airports, hotels).
- Pick the fastest nearby location for best speed.

2) Passkeys / Manager

- Import passwords into a password manager or setup **passkeys** for apps.
- Use strong, unique passwords for the rest; enable **2FA (2 factor authentication)**.
- Share credentials with VAs via the password manager (no plain-text DMs).

3) Threat Protection

- Turn on malicious-site, tracker, and download blocking.
- Test: Try a benign phishing-test URL—confirm it gets blocked.
- Keep a “suspicious links” rule: when in doubt, open in a sandboxed browser.

The 2 Rules

1) Use non-admin accounts for daily work.

- Limits malware and account highjack access to your system and data.

2) Backups - Onsite and offsite storage.

- Ensures quick recovery - data loss no longer means losing your business.

Troubleshooting & Tips

Speed feels slower?

- Switch to closest server & ensure **WireGuard-based** protocol.
- Close heavy background uploads (cloud sync) while on untrusted Wi-Fi.

App won't log in?

- Toggle VPN off → log in → toggle back on (first-time handshakes)**.**
- Add the site/app to your security manager trusted list and enable 2FA.

Shared devices or VAs?

- Use a separate OS profile/accounts (non-admin) for each person.
- Share access in your security manager; revoke access if roles change.

Backups

- Keep work files in a synced folder with version history.
- Snapshot weekly to external or cloud storage (for safe offsite storage).

Proof & ROI – what this actually saves you

Small wins creators actually feel

- Kill Switch + Threat Protection can detect and stop sketchy public Wi-Fi redirects during client work.
- A password manager ends the weekly "forgot password" spiral and the risk of simple, reused passwords.

Cost of doing nothing (example month)

- ***2 hours lost to resets and phishing clean-ups*** → if your time is worth **$50/hour**, that's **$100**.
- ***One client refund or account mix-up dispute*** → even a **$150** refund wipes out profit.
- ***2 hours downtime from sketchy Wi-Fi*** during a launch or client deadline → another **$100**.

Total example cost: ~ $350 in stress/lost income from security problems.

Now compare that to:

- What you pay per month for a solid VPN + threat protection + password manager stack (often less than a couple coffees a week), and
- 10–15 minutes of setup using this checklist.

If this setup prevents even **one** bad month like the example above in a whole year, it has already paid for itself.

To Start Now - Choose your path...

- **Complete** = encrypted browsing + malicious-site blocking
- **Prime** = **Complete** + password manager & secure storage locker
- Setup time: ~10–12 minutes

Get Prime **Get Complete**

© Borderless Digital Shield™ · Privacy and Terms

Disclosure: I may earn from links at no additional cost to you.

Borderless Digital Shield™
- Work-Anywhere Wi-Fi Shield

Why this matters

If your business fits in a backpack, your “office” is whatever Wi-Fi you’re on right now.

Airports, hotels, and coffee shops are convenient—but they’re also places where attackers quietly watch logins on fake or insecure networks.

Rule #1 · No VPN = No logins

If a network isn’t yours, your VPN should be ON before you log into anything.

On open networks and public Wi-Fi, do NOT log into:

• Business email

• Stripe, PayPal, banking

• Store or ad dashboards

…unless your VPN is connected and stable.

New habit: “No VPN = No logins.”

Rule #2 · Be picky about “free Wi-Fi”

Fake “FREE_AIRPORT_WIFI” is a real thing.

Before you connect:

• Ask staff for the exact Wi-Fi name

• Avoid weird spellings and look-alike networks

• If anything feels off, tether to your phone for email + money work

Rule #3 · Business-only browser

Create one browser/profile used only for:

• Business email

• Money tools (Stripe, PayPal, banking)

• Store dashboards and client systems

Rules for that browser:

• Only open it when your VPN is ON

• Use a password manager + 2FA for every login

• No random browsing or social scrolling

Quick self-check

In the last month, have you:

• Logged into Stripe/PayPal/banking on unsecure/public Wi-Fi with no VPN?

• Connected to “free” Wi-Fi without checking the name?

• Used the same window for TikTok, Stripe, and client dashboards?

If yes, start with one change: “No VPN = No logins” on public Wi-Fi.

Borderless Digital Shield™
- Work-Anywhere Payables Safety Card

Why this matters

If you pay contractors, designers, VAs, or vendors by bank transfer, one rushed email approval can send money to a scammer.

Once it’s gone, it’s usually gone.

Step #1 · Pick your pain number

Your pain number = the amount of money that would really hurt if it went to the wrong place.

• $300? $500? $1,000+?

Any payment at or above that number:

• Never happens on autopilot

• Always gets slowed down and double-checked

Step #2 · Bank changes = phone calls

“We changed bank accounts” should feel like a fraud alert.

When you see new bank details:

• Don’t approve from email alone

• Call a saved number you already had on file

• Confirm bank name, routing, and account number

Step #3 · Two-eyes rule

Over your pain number, no single tired brain moves money.

• Get a second person to review, or

• Review it yourself again after a break

Check: vendor, amount, bank details, purpose.

Step #4 · Approve from your safe space

Big money decisions don’t belong in your inbox on public/open Wi-Fi.

Approve invoices only from your:

• Private Business Space (business-only browser)

• Behind your VPN.

Borderless Digital Shield™
- Work-Anywhere Ransomware Shield

The risk

A 158-year-old company shut down for good after attackers found one public login with a weak password and no 2FA (Two-Factor Authentication).

No movie-style hacking—just an easy password on a wide-open door.

Step #1 · Strengthen your “front doors”

Your front doors are:

• Store admin (Shopify, Etsy, Woo, etc.)

• Stripe / PayPal

• Hosting / server panel

• Email admin

Put them in a password manager and give each a long, unique password.

Step #2 · 2FA where it hurts most

Anywhere money moves or settings change:

• Turn on two-factor authentication (2FA)

• Prefer authenticator apps or a security key over SMS codes

Step #3 · Admin logins from your safe space

Only log into:

• Store admin

• Stripe / PayPal

• Hosting

• Email admin

From your Private Business Space, behind your VPN.

No more admin logins on open/raw networks or hotel/coffee shop Wi-Fi.

Step #4 · One backup you can trust

Decide what you can’t afford to lose:

• Key files

• Product data

• Critical documents

Keep at least one encrypted backup off your main device—and test it periodically.

Borderless Digital Shield™

- Work-Anywhere IG Shield

Why this matters

If IG or TikTok brings you customers, that handle isn't a hobby—it's your storefront.

If attackers hijack it, they can use your face and posts to scam people you care about.

Step #1 · Separate IG + email passwords

Give IG and the email tied to IG their own long, unique passwords in a password manager.

Never reuse these passwords anywhere else.

Step #2 · 2FA + backup codes

Turn on 2FA (Two-Factor Authentication) for:

• IG

• The email connected to IG

Generate backup codes and store them:

• Offline

• Somewhere only you can access

• Not inside your inbox.

Step #3 · Logins from your safe space

Treat IG and other business social media like your storefront:

• Only log in from your Private Business Space

• Always behind your VPN

• Avoid logging in from random, open hotel/coffee shop Wi-Fi.

Quick self-check

Ask yourself:

• Are IG and the email tied to it using different, strong passwords?

• Is 2FA (Two-Factor Authentication) enabled for both?

• Do you know where your backup codes live?

Borderless Digital Shield™
- Work-Anywhere Creator Shield

The real risk

Your audience will trust your link more than any warning label.

If your account is hijacked, that trust can be used to run fake giveaways and offers in your name.

Step #1 · One password per platform

Put all your platform logins into a password manager:

• IG / TikTok / etc.

• Email

• Link-in-bio tool

• Course / offer platforms

Give each one its own, long, unique password.

Step #2 · Slow down on “support” / “verify” links

When you see messages like:

• “Verify your account”

• “Your payout is blocked”

• “Your page will be removed…”

Assume phishing first:

• Don’t log in from the link

• Open the app or type the URL yourself

• Check alerts inside the platform.

Step #3 · Edit link-in-bio from your safe space

Only change:

• Link-in-bio

• Money-related links

From your Private Business Space, behind your VPN, on a trusted device.

Quick self-check

Ask yourself:

• Are you reusing a password on more than one platform?

• Have you logged in from a “verify/support” link before?

• Do you edit link-in-bio from random networks/devices?

Borderless Digital Shield™

- Work-Anywhere Platform Shield

Who this is for

Gig workers, drivers, delivery partners, Etsy/Amazon sellers, freelancers

— anyone whose income flows through big apps and platforms.

Step #1 · Single-use passwords

Put your email and each platform login into a password manager.

Give each its own password.

One stolen password should not unlock everything else.

Step #2 · Dashboards in your safe space

Only open:

• Dashboards

• Payout settings

• Account management screens

- - from within your Private Business Space, behind your VPN.

No managing payouts from random email links and/or on open networks such as public Wi-Fi.

Step #3 · Inbox links are guilty first

When you get a message saying:

• “Update your account”

• “Confirm payout info”

• “Your account will be closed…”

Treat it as phishing until proven otherwise:

• Don’t log in from the link

• Open the real app/website directly

• Check for alerts there.

Quick self-check

Ask yourself:

• Are you reusing passwords across apps?

• Do you manage payouts from email/text links?

• Have you opened dashboards on public Wi-Fi with no VPN?

Borderless Digital Shield™

- Work-Anywhere Scorecard & Next Steps

Score yourself (0–2) - For each area, give yourself a score:

0 = Not in place 1 = Partially in place 2 = Solid

Areas to score:

- Work-Anywhere Wi-Fi Shield
- Payables Safety
- Ransomware Shield
- IG Shield
- Creator Shield
- Platform Shield
- Private Business Space habits

Your next 3 moves - In the next 48 hours, I will change:

1. _____
2. _____
3. _____

Start with your highest-risk area for business (Wi-Fi, money, or storefront).

Weekly check-in

Once a week, ask:

- Did I log into money | client systems on unsecure/public Wi-Fi minus VPN?
- Did I approve any big payments without a second check?
- Did I reuse a password anywhere new?

If yes, go back to the matching card and fix that first.

Get help / Stay updated

If you want help turning this into a simple routine:

- Comment or DM “TEACH ME” on Instagram
- I’ll send you the latest Borderless Digital Shield™ toolkit link
- I’ll share new, real-world stories and fixes as attacks change.

To Start Now - Choose your path

- **Complete** = encrypted browsing + malicious-site blocking
- **Prime** = **Complete** + password manager & secure storage locker
- Setup time: ~10–12 minutes

Get Prime **Get Complete**

© Borderless Digital Shield™ · Privacy and Terms

Disclosure: I may earn from links; no extra cost to you.