Bulletproof Online: The Anti-Scam Playbook - Part 1: The Internet Survival Kit

The "Bulletproof Online" series begins with Part 1: The Anti-Scam Playbook, providing essential tips to navigate and protect yourself from scams in the digital world.

Stay Safe from Online Scams: Phishing, Fake Ads & Social Tricks

Scammers are smart. They use phishing emails, fake ads, and pop-ups. Most importantly, they use social engineering to fool you. They do all this to obtain your passwords, credit cards, or simply persuade you to click on malware. It occurs on a daily basis, without exaggerating the impact. One report noted that 80–95% of all cyber breaches start with a phishing email or similar scam **(**hoxhunt.com). Americans lost more than $10 billion to fraud in 2023 **(**ncoa.org), and criminals are becoming bolder. A UK investigation in early 2023 caught scammers in the act of using deepfake celebrity ads on Facebook and Google (fake videos of Martin Lewis and others), pushing bogus crypto investments the (theguardian.com).

You should always suspect unexpected messages even when they appear real. View link URL (on a computer) by hovering over it or, preferably, go directly to the official site (not via the email). Avoid urgent requests. Legit companies don't say "act now or lose out" or "you'll be sorry!" by email (ncoa.org). The example of a 90-year-old woman who lost $20,000 to a scam by a fake tech-repair joint, is quite common. Imposter scams cost Americans $2.7 billion in 2023. This includes people pretending to be your bank, IRS or loved one in trouble (ncoa.org).

Tips & Action Steps

• Be cautious when receiving unsolicited requests for your password, social security number, or other sensitive information. Legitimate businesses won't send random demands. Instead, close the message and contact the company yourself. For example, if it states that you have "got a refund," give the phone number a call, and you should hang up and instead call the real number of the company. One expert suggests closing the email and manually visiting the company's official website or contacting them for verification *(*quickbooks.intuit.com)..

• Watch out for warning signs, like generic greetings ("Dear Customer"), misspellings, or strange addresses of the sender. Be cautious if the email copy-pastes a logo but asks you to click a link or to open an attachment (consumer.ftc.govtitanhq.com). According to TitanHQ, fake invoices and shipping notifications will come with a malicious attachment. Always check those on the official site, not by clicking (titanhq.com).

• Be sure to protect yourself from malicious links and website phishing attacks by utilizing security software and spam filters on your email. Ensure you install trustworthy security software on your devices and upgrade it. The ads from this software are safe, providing you with extra protection against malvertising that can infect your computer simply by loading a web page.(csoonline.comcsoonline.com).

• Report scams: Don’t ignore emails, pop-ups or texts that seem suspicious—report them to the experts. U.S.-based readers can report to FTC.gov/reportfraud or the FBI’s IC3.gov scam reports. (NCOA advises the elderly to promptly inform the FTC of fake contact attempts ncoa.org.).

A healthy amount of skepticism, along with using spam filters and updated browsers, will keep most phishing attempts at the door (consumer.ftc.gov). If an offer appears excessively favorable or frightening, it's likely not genuine!

Stay Safe from Smartphone Scams: Malicious Apps, Fake Calls & Smishing

Crooks are aware that a smartphone is like a powerful computer in the pocket. Scammers are now targeting phones with “smishing” (SMS phishing) texts, bogus app downloads, and scam calls more than ever. In April 2024, the FBI issued a warning about text messages impersonating a toll company and claiming “unpaid tolls.” However, the link actually led to a phishing site that stole money and information (ibm.com). During the holiday seasons or tax time, you may receive a message regarding a “delivery issue” or “tax refund.” These are often smishing scams that could lead you to click suspicious links.

Scammers also make fake calls, “vishing,” where they put on a false persona of an IRS agent, tech support, or a relative in trouble. According to NCOA, seniors lost $1.3 billion only to tech-support scams in 2023 (ncoa.org). One tactic involves the caller claiming to represent Microsoft. They demand payment—often through gift cards. They do this so they can “fix” your computer. If someone calls you out of the blue and claims to be tech support or the government, just hang up. Fraudsters can fake phone numbers to make calls appear legitimate, in a practice known as “caller ID spoofing.”

Malicious apps are another mobile threat. Official app stores may not be that safe either: in 2024, Google blocked 2.36 million harmful Android apps and banned 158,000 developer accounts (thehackernews.com).But some sneaky spyware slips through. Here is a paraphrase for that sentence:

Security researchers have found that a hidden malware known as SparkCat may be present in some iPhone apps. It can read your screenshots to steal your crypto wallet password (theverge.com).

On Android, apps sometimes bundle malware or adware. Researchers discovered in 2024 that a large influx of fake VPN apps on the Play Store contains malware (tomsguide.com).

Tips & Action Steps

• Only download apps from official stores, like Google Play and Apple’s App Store, and preferably with a favorable reputation. Beware of random “free” apps or games that seem popular. If an app asks for too many permissions (for example, a flashlight app asks for access to your contacts or camera), revoke permissions or uninstall as it is suspicious.

• Turn on Protect Android, and keep Google Play Protect on (it automatically scans apps for threats) ((thehackernews.com). On iPhones, keep your device's built-in security (do not jailbreak your phone). To catch malware on an Android phone, install a reliable mobile security app.

• Keep Your Operating Systems Up To Date: Phone operating systems, like computer software, get security fixes too. Install the latest updates for iOS or Android as soon as they are released—they often close loopholes hackers try to use.

• Screen your calls and texts: Don't trust unknown callers. Let voicemail filter out spam calls, or use built-in spam-call warnings. And do not ever click a link from an unsolicited SMS – for instance, if you get a text that claims to be from UPS, go to UPS's official website yourself to check on your package. The IBM security team says hackers often use customer support or delivery company messages (ibm.com) to lure victims.

• When you get a scary call or text (like your "bank" is calling to tell you there is fraud) hang up and call your bank using the phone number on your statement to confirm. Never call any number they give you for tech support pop-ups. Instead, trust your knowledge or search online.

• It can be beneficial to use two phones—one strictly for banking or crypto and one for your day-to-day use. This way, clicking a link on the "junk" phone won't impact your crypto wallet since it is on another phone.

Despite being powerful, modern smartphones can be attacked in many ways. Staying within the official channels and rechecking everything from a different device or website can save you from most scams on your mobile. When your phone screams "DANGER." at you, it's not hawking a hot new app. This is merely a helpful reminder to keep in mind.

VPNs Explained: What They Are and How to Choose One

Perhaps you have heard of VPNs (Virtual Private Networks), especially if you're into crypto or just like your privacy. But what is a VPN, exactly, and do you need one? A VPN is a service that provides an encrypted connection to the Internet (security.org). It also hides a user's real IP address. How does a VPN work? When you use a VPN, all your internet traffic is sent to that VPN company's server through a "tunnel." Your internet traffic then gets sent to the web using the VPN company's IP address instead of your own. (security.orgsecurity.org) This technique means outsiders (including hackers or your ISP) see only encrypted gibberish. In other words, the websites you visit see only the VPN server's IP, not yours. (security.org) People utilize VPNs to keep data safe on public Wi-Fi, browse without being tracked, and access restricted websites.

But not all VPNs are created equal. Here's how to pick a good one.

• Choose a VPN that uses top-notch encryption (AES-256 or OpenVPN/WireGuard protocols). It scrambles your data so effectively that, even if it is intercepted, nobody can read it.

• A reliable VPN should not log data and sell it. According to security.org, the privacy policy of your provider should state that they do not keep web activity records nor records of your IP address. To put it another way (42 words): Some lesser VPNs might log and sell your info to advertisers. Ever since, experts have warned that many free VPNs track you. One estimate states 80% of free VPNs will have tracking by 2025, and 60% will sell user data (tomsguide.com). So be cautious of “free’ services; you usually get what you pay for.

• Choose a VPN provider that has a good reputation and location. Select a VPN from a reputable entity (e.g., ProtonVPN, NordVPN) that has been audited or reviewed. Pay attention to the location of a company’s headquarters. Users usually go for companies that aren’t based in “surveillance alliances,” as that protects them from data handover (security.org).

• Kill switch: A trustworthy VPN has a “kill switch” feature (security.org). When your VPN drops, the automatic kill switch blocks internet access to prevent any data leak. Always keep the kill switch on.

• Trust and purpose. Know why you need a VPN. For basic privacy on public Wi-Fi, any decent VPN is fine. If you need speed, look at reviews for fast providers. If you wish to unlock streaming or particular countries, choose a VPN with the right servers. Refer to the NSA/CISA VPN guide (for tech types) and good old VPN review sites for more comparisons.

To use a VPN safely, install the VPN app from a trusted source (official website or app store). Always bear in mind the location/server you connect to: that’s your online location. Enable the kill switch (and auto-connect if it is available) so your traffic is always protected. Even the best VPN won't preserve your identity. If you use a VPN, you still log in to your accounts in the normal way. Scammers can still phish your credentials.

A VPN is a secure tunnel for your data. (security.org) Using a VPN is a fantastic way to secure your internet traffic. However, exercise caution when selecting a VPN, preferably one that is paid or at least not free, to avoid falling victim to the deceptive nature of "free" VPNs (tomsguide.com). If you're not sure who to trust, one step is to read reviews.

Email Security Tactics: Spam Filters, Link Checks & Verifying Senders

Scammers love email and target it very often for phishing schemes. But your inbox has helpers! Your email provider (Gmail, Outlook, Yahoo, etc.) uses filters to catch spam and phishing emails so you never see them (at least not in your inbox). Your email spam filters may block many phishing emails from reaching your inbox (consumer.ftc.gov), according to the FTC. Always keep those filters active and periodically check your folder for any lost doses of emails.

Even with filters, stay alert with every message you do see. Be cautious before clicking on any links or downloading any attachments.

1. Don’t trust the displayed name easily. Check the sender. Hover (on a computer) or tap the sender’s address to see if it’s a weird email (e.g., something@gmail.com when the sender claims to be “Your Bank”). If it doesn’t match the real website domain, it’s fake.

2. Move your mouse over a link on your computer to check the real address of that link. Is it slightly misspelled (e.g., go0gle.com instead of google.com)? If you're on mobile, try pressing and holding to see link info. Don't click if it appears incorrect. (titanhq.com) Please visit the official site directly. For example, a fraudulent "invoice" email might lead you to a convincing site that's actually a trap. Logging into your account in your browser is safer than using links sent to you over email.

3. Be careful about opening attachments. The attachments contain malware. If you get an unexpected invoice PDF or image file, pause. (titanhq.com) A legitimate company will never send you an unexpected attachment. It's safer to check by logging into your actual account at the company's legitimate site (e.g. your credit card or bank site) than to double-click the file. According to a tip, it is best to visit the official website to access information instead of clicking on email links or downloading attachments.

4. Be aware of the use of an urgent or scary tone: "Your account will be shut down!" "Virus detected!" If you didn't make the request or expect the message, be sure to be suspicious (quickbooks.intuit.com). of the QuickBooks security guide. For example, tax scams and IRS scams rise during filing season: the IRS will never demand money by email or require you to send gift cards.

Tips & Action Steps

- Setting up your email with two-factor authentication limits the access an attacker can get with just your password. (More on 2FA below.).

- Ensure your browser and extensions are updated, as some phishing websites exploit browser vulnerabilities. To minimize risk, you should update your browser and disable unnecessary plugins.

- You can report phishing emails to services like Gmail. Most email services allow you to report spam or phishing with a click (or tap on that three-dot menu). If the scam sounds serious, consider forwarding it to a government site (e.g., FTC's ReportFraud). This procedure helps authorities shut down bad sites.

You can protect your email with a combination of excellent instincts and basic tools (spam filters, careful clicking). Those bogus messages can appear to come from your bank, a delivery service, or various other institutions. As the FTC says, scammers "send thousands of phishing scams like these every day" (consumer.ftc.gov). But you can trick these scammers before you click if you check the link and the sender before you act.

Smartphone Security Habits: Apps, Updates & Antivirus

Let's secure your device so it's harder to attack or access your personal information in the first place. Safety advice online also applies to phones with a few twists and turns, though.

• After installation, check what permissions the app has (camera, microphone, contacts, etc.) and manage it. On Android, go to Settings ➔ Privacy ➔ Permission Manager. Examine each app's settings on your iPhone. Please consider disabling any features that appear unnecessary. A flashlight app should not request access to your location or contacts. When an app demands all the permissions suddenly, revoke or uninstall the app.

• Automatic updates: Enable automatic updates of your phone's system and applications. Constantly released patches address security bugs. For Android, access Settings ➔ System ➔ Advanced ➔ System update. On iPhone, Settings ➔ General ➔ Software Update. It's safer to have a phone that is up to date; several malware infections take advantage of old security holes.

• Scan your apps using the built-in antivirus/scan option. On Android devices, you can ensure that Google Play Protect is enabled. (thehackernews.com). (Launch the Google Play app, tap on your avatar, and select Play Protect. For iPhone, while the app review process by Apple is strict, caution is still advised against any suspicious profiles or certificates (most users never need third-party iPhone antivirus). It's best to avoid jailbreaking or rooting your phone, as this disables many protections.

• Always set up a strong passcode or fingerprint/FaceID lock on your sensitive apps (banking, email, crypto wallets). Many apps, such as banks or password managers, allow you to set up an extra PIN on top of your device lock. By doing this, you won't be able to open those apps even if someone else unlocks your phone.

• Make regular backups of your phone data (to the cloud or your computer) and activate device encryption (usually on by default). This is to ensure the safety of your data in case your phone is lost or stolen.

• Be cautious about charging cables: It may sound strange, but "juice jacking" is a thing — a public USB port can infect your phone with malware. Use your own cable and a power-only adapter, or just the outlet, when charging in public.

It only takes a couple of bumpers to set up these habits, but they go a long way. Locking your phone down is key; in fact, Lookout's 2023 Mobile Threat Report warns mobile phishing is exploding and vulnerabilities are rampant (lookout.com). When your device is updated and your apps are vetted, even if a fraudster tricks you once, at least the walls of your phone are high.

Strong Accounts & Password Security: 2FA, Managers & Passphrases

Finally, let's shield your accounts. Make sure that all passwords you use are forceful and unique. Add additional layers of protection if you can.

• If you're having difficulty remembering dozens of passwords, a password manager (like Bitwarden or 1Password) can certainly help. They can also generate long random passwords such as "MyC@t7ZiGwn$" and save them. Around 36 percent of the American people use a password manager (security.org) for stronger security, and if they do, they will get hacked quicker (security.org). This is excellent news: password managers prevent reuse; this is because nearly 20% of people reuse the same password for multiple accounts. New FBI data shows that Americans lost $16.6B to schemes in 2023. One common problem is reused passwords (abcnews.go.com). A password manager stops that.

- Make sure to set up two-factor authentication everywhere. Having 2FA (two-factor authentication) means there is something extra you need beyond just your password, like a code, your fingerprint and more. Enable 2FA on your email, bank, social media—and yes, crypto accounts. According to Google, even a basic 2FA, like a simple authentication code sent via text message, stops 100% of automated login attacks and 96% of bulk phishing efforts.(techcrunch.com)For maximum protection, choose an authenticator application like Google Authenticator, or even better, get yourself a hardware key for those really sensitive accounts. The point is the same: with 2FA turned on, a stolen password won't be enough for a scammer.

- Use a mix of numbers, symbols, and double-digit letters; use password managers, and do not reuse passwords. A phrase that consists of multiple words, like "BlueMonkey$Coffee88!", can be difficult to crack. Steer clear of easy replacements (Pa$$w0rd! is still a weak password), and don't use personal stuff, like your birthday and pet name. The data suggests that bad habits are risky: 37% of people admit to using the same password on many sites (explodingtopics.com), and 13% use the same password for everything (explodingtopics.com). Don't be that just 13%—when one site gets breached, all the accounts that share that password are exposed.

- "Do you have old email or shopping accounts you no longer use? Update or delete.". If applicable, please delete them or update those passwords. Hackers prefer untouched accounts because they lack adequate security.

- Ensure you log out of the browser after completing your work on shared PCs. In a public PC (like in a library, hotel business center, etc.), never allow the browser to "remember" you. Make sure to sign out and clear the cache so that no one clicks into your accounts.

Quick Tips

- Whenever possible, opt for Gmail Authenticator or a similar app for two-factor authentication instead of SMS.

- Turn on two-factor authentication (2FA) for your email first. If someone hacks your email, they can simply reset all of your other passwords.

- Every once in a while, check if your passwords are compromised (services like haveibeenpwned.com can tell you). If you find one, make the necessary changes right away.

Investing a small amount of time and effort in setup is a highly effective defense. Accounts are your passwords to everything, so remember to lock them!

What's Next? (Hint: Crypto & Blockchain Security!)

Well done! You just created a powerful shield against online scams. By now, you know how to thwart phishers, dodge app and call scams, smartly get a VPN, and eventually lock your email and phone and enhance your accounts.

In Part 2 of this series, we'll explore advanced scams and blockchain security: fake wallets, scam coins, SIM swaps, and beyond. For now, keep the following practices in mind and share them with your friends and family (especially your tech-challenged grandma). We all need to outsmart the fraudsters to make the internet a safer place for everybody!