Digital Security

Your Personal Protection & Online Privacy Guide for 2022

Digital security is a confusing and overwhelming topic for the average person.

Between all the industry jargon, vast selection of online privacy tools, and regularly occurring data breaches — it's easy to feel disconnected from this space.

After reading this guide, you'll have a clearer understanding of digital security and how to defend yourself against the endless array of vulnerabilities and online threats that exist today.

What Is Digital Security?

Digital security aims to protect your devices, personal data and online identity from external harm on the internet. It includes all the tools, techniques and security training that keeps you safe online.

Your life online is an ecosystem of information systems, data, behaviors, and tools which are constantly interacting with each other. Ultimately, this is what makes up your digital footprint.

Cyber security experts and innovators around the world are developing advanced digital security solutions to fight back against the overwhelming volume of cyber attacks happening on the internet.

What Should I Expect from a Digital Security Suite?

1. Device protection
2. Network security
3. Identity theft protection
4. Credit monitoring
5. Antivirus software with VPN
6. Secure password manager
7. Dark web monitoring
8. Social security monitoring
9. Parental controls
10. Family protection

The goal of comprehensive digital security is to provide you with an easy-to-use solution that safeguards all aspects of your online activity.

Cyber Security vs. Digital Security: What's the Difference?

Cyber security incorporates every proactive and reactive method of preventing illegal access to a person's devices, data, accounts, identity, and finances.

It’s a complex field that ensures information security for all technical components and their interactions with humans.

This includes computer networks and systems, devices connected to them, the sensitive information on those devices, and many other layers of technology we (mostly unconsciously) use every day.

As a subsection of cyber security – digital security focuses on protecting your digital identity, meaning your online activities and the data they produce.

Why Is Digital Security Important?

Unfortunately, we see, once again, that people over 60 suffer the most from internet scams and cyber attacks.

Because senior citizens are so vulnerable to fraud, digital security is absolutely imperative for their stability and wellbeing.

Hackers view your digital identity as a source of income (e.g. online shopping, social media activity, browsing history, etc.) Scammers will isolate targets with weak or nonexistent security systems to steal (or extort) your money.

Repeatedly, we’ve seen people realize the importance of investing in their digital security through new tools and safer habits. Unfortunately, this change in attitude and behavior often comes after falling victim to a data breach.

According to a Survey by Propeller Insights, after a cyber attack:

- 61.6% of people become more cautious about the information they share online.
- 50.8% of people become more cautious about using new payment technologies.
- 48.6% check their credit report.
- 40.7% sign up for an identity theft program.
- 35.6% investigate who they do business with online.

What Types of Hackers Are After My Data?

Believe it or not, there is something called ethical hacking.

Ethical hacking involves using specialized techniques to find and test vulnerabilities in computer systems so they can report, fix, or adequately protect information systems from bad actors with malicious intent.

Here are a few helpful distinctions between different types of hackers:

- A white hat hacker uses ethical hacking to help secure computer systems and keep technology safe.

- A black hat hacker (also called bad actor, threat actor, and malicious hacker) uses their hacking knowledge and skills to gain illegal access, data, or money from systems and people they victimize.
- A gray hat hacker, as the name suggests, operates in a gray area, sometimes combining good intentions with not-quite-legal methods.

Ethical hackers (white hats) assume the attacker's perspective and pass on remediation details to those tasked with fixing the issues—from software developers to business executives. That's because they share the same responsible objective: keeping the internet safe for everyone.

Black hats, however, have more nefarious motivations. They often seek to get large amounts of money fast or pull off ego-boosting hacks that inflate their reputation in the cyber crime world.

Some of them create, sell, or rent malicious hacking software and infrastructure to launch cyber attacks. Certain malicious hackers even work in state-run cyber warfare operations such as WannaCry or Petya and NotPetya.

What Are the Main Types of Cyber Attacks?

There are three main types of cyber attacks that can affect you and your loved ones.

Spray & pray attacks

These attacks target a huge number of people (i.e. millions) and are mostly automated.

Spray & prey attacks guarantee "good coverage" even with a tiny percentage of victims.

Tactics include phishing emails, malware attacks, websites that distribute malicious code, and links that trigger ransomware infections.

Targeted attacks

This type of malicious hacking focuses on a specific asset and uses personalization to extract access, data, or money from unprepared victims.

A common example is smishing, which targets people with infected or phishing links through seemingly authentic texts that incentivize the victim to share their financial information (i.e. credit card details).

Advanced persistent attacks

APTs, as they're abbreviated, use detailed research and planning to gain access to a big target with multiple goals that all end in a big payout.

These may not target you directly, but they affect the organizations whose products and services you use.

While inside the network, attackers collect data about how the organization works and plant malicious software that enables them to launch attacks at a later time.

The ultimate goal is to sell the data (including yours) for a big return or extort the company by threatening to expose it.

These types of cyber threats have both immediate and long-term impact on your digital security.

In the short term, you either lose data or money (or both), and sometimes get locked out of your accounts and devices.

Long-term consequences come from how scammers use the data they gather about you from voluntary and unintentional personal information sharing.

Digital identity theft is one of the most taxing repercussions, both financially and emotionally.

Common Digital Security Threats

Unlike driving, using the internet doesn't come with any form of security training that teaches proactive protection.

Unsecure Access

There are two things that make it ridiculously easy for attackers to access your online accounts:

- Using weak passwords and reusing them for multiple accounts.
- Not enabling two-factor authentication.

Without these important forms of access control, it's substantially easier for malicious hackers to breach your accounts. Once inside, they collect more data, use your contacts to find additional victims, and even take over your accounts to sell them.

For example, a Netflix account with a one-year subscription gets traded for $44 on the dark web.

Dangerous Exposure

Your digital identity enables hackers to form a very clear image of who you are, what you do and when, what you like, and how much money you might have.

Imagine your privacy is like a puzzle. The more pieces of your personal information that are found on a public domain, the easier it is for cyber criminals to put them together.

The average person has over 100 online accounts[*], which means your information spreads on the internet and well beyond — in systems that store your personal data for long periods of time which you have no control over.

Plus, the volume of information we deal with on a daily basis erodes our ability to pay attention to details and correctly assess risky situations. The less attention you pay to these safety gaps, the more detrimental this becomes.

So, It's a good idea to do a personal data exposure test to get a sense of how far-flung your confidential information is.

Too Many Devices

From laptops and smartphones to IoT devices like smart doorbells and home assistants, all sorts of internet-connected devices have become part of our lives. The data on these devices, along with their operating systems and apps, expand your attack surface (the total number of points an attacker can use to gain illegal access).

Without proper security measures and maintenance, even less skilled attackers can trigger a devastating domino effect. One of our employees went through a terrible ordeal in his pre-Aura days, when someone stole his smartphone and took over all his main accounts, costing him $12,000.

Psychological Manipulation

Malicious hackers are not just adept at exploiting technology and personal data. They also know what triggers people to react, including fear and surprise.

That's why you should be aware of the common warning signs of typical online scams, like:

- Suspicious login attempts
- Unrecognized devices
- Data breach email alerts
- Unfamiliar charges on your financial statements
- Unfamiliar remarks on your credit report

How Does Digital Security Work?

We've created a checklist for building a strong personal protection and online privacy ecosystem, including timeless principles for enhanced digital security in 2022 and beyond.

1. Prioritize:

- Make a list of your most important digital assets.
- Review your personal exposure levels on mobile devices, online accounts, and apps.
- Determine where your social security number, healthcare insurance details, driver license info, etc. may be revealed.

2. Protect:

- Invest in products and services that cover both your digital security and online privacy.
- Consider solutions that protect your local data (on your devices) and on the internet (publicly available personal information).
- If you want to easily extend that protection to your loved ones, look for family identity theft protection.

3. Monitor:

- Set yourself up for success with fraud alerts that notify you of suspicious activity.
- Use alerts to keep track of your exposure, gradually limiting it with caution or by expressly deleting data to which you have access.

4. React:

- Take swift and decisive action to protect your privacy and security when you receive alerts.
- Be vigilant when you buy new devices or sign up for new services.
- Regularly review your credit report and financial statements for suspicious activity.

The Aura Digital Safety Ecosystem

Protect	Monitor	React
Antivirus software for all your devices.	Identity monitoring.	Lost wallet remediation.
Wi-Fi Security for your home network.	Credit monitoring.	White glove fraud resolution.
VPN for encrypted communication when you connect to public Wi-Fi.	Dark web monitoring.	$1M identity theft insurance.
Password Manager for strong and secure credentials.	Transaction monitoring.	24/7 U.S. based support.
Identity theft protection extended to your whole family.	3-credit bureau monitoring.	Instantly lock your credit.
Social security number protection.	Home title monitoring.	Dispute fraud immediately.

Which Digital Security Tools Can Protect Me from Getting Hacked?

- Device security (i.e. antivirus software) to ensure your smartphone, laptop, tablets, and other gadgets are safe to use, no matter their operating system (iOS, Android, Microsoft Windows, etc.)
- Internet traffic filtering and encryption that automatically blocks cyber threats posed as legitimate data transfers.
- A password management feature to make creating and using passwords substantially easier and safer.
- Dark web monitoring to get alerts when scammers and malicious hackers try to trade or use your personal details in the farthest corners of the internet.
- Identity theft protection for extensive monitoring of your personal information, accounts, IDs, and other sensitive data that bad actors can use to defraud you.
- Financial fraud protection, including credit monitoring, to get near–real time alerts when new inquiries on your credit file pop up (e.g. new credit cards or bank loans) or when suspicious spending activity suggests your financial assets may be in danger.
- Parental controls that limit the amount of time your kids spend online. Parents need the ability to restrict screen time, block certain apps and websites.
- Great customer service to help navigate a critical situation such as losing your wallet (and the sensitive documents in it) or just making sure you're maximizing the benefits of your security suite.
- The option to extend all of these features to your entire family and their devices.

Ultimately, your digital security toolbox is more effective when a single, trustworthy service provider supplies the various security layers you need.