Bitdefender®

DIGITAL IDENTITY PROTECTION

USER'S GUIDE

Bitdefender Digital Identity Protection
User's Guide

Publication date 03/24/2020

Legal Notice

Bitdefender

Table of Contents

1. WHAT IS BITDEFENDER DIGITAL IDENTITY PROTECTION

Online privacy and security are some of the main focuses for internet users nowadays. And there are some very good reasons for that. With major data breaches happening more often than not, it is imperative to make sure that your personally identifiable information (PII) is safe and secure.

But what can be classified as personally identifiable information? Traditionally, sensitive information such as the full name, social security number, driver's license, mailing address or credit card information were considered PII. Eventually, less-sensitive info, such as zip codes, IP addresses, or login IDs were also included. Over time, your digital footprint, meaning the data you leave behind as a result of your browsing the internet, might come to include some of these.

Bitdefender Digital Identity Protection represents the private way to online freedom, allowing you to regain control of your digital life. And it requires only your name, most used email address and your phone number. Based on these, it searches on both the Surface Web and the Dark Web for personal information that was exposed publicly.

Bitdefender Digital Identity Protection offers the following:

- **Monitoring and detection services**: it monitors more than 100 personally identifiable information such as SSN, credit cards or home address, and displays all data found about your online footprint.

  Note
  Bitdefender does not store or process personally identifiable information. Only references to potential data breaches are kept, without including sensitive data.

- **Real-time alerts**: You receive notifications about data breaches and exposed data in Dark Web, personal information in Surface Web and potential impersonators you on social media.
- **Solutions**: Our service suggests clear actions required to solve issues and provide reminders if an issue is not solved entirely. It can also provide instructions on how to remove the personalized ads, export your data, or turn off the tracking.

  .

2. GETTING STARTED

Configuring Bitdefender Digital Identity Protection

1. Go to https://central.bitdefender.com/ and sign in to your account.

   If you don't already have an account, click on **CREATE ACCOUNT**, then type your full name, an email address and a password.

2. Select the Digital Identity Protection panel.

   A welcoming screen is displayed.

3. Click **BEGIN**.

4. You will now be informed on what information you need to provide. Your data will always be encrypted and secured.

   Click **NEXT**.

5. Type your first name, middle name (if any) and last name in their corresponding boxes, then click **NEXT**.

6. Type your email address, then click **NEXT**.

   Make sure it is a valid email address you can access.

7. A security code is sent to the address you provided.

   Open your email, copy the code and paste it in its corresponding field.

   After that, click **CHECK**.

8. Select your country and enter your phone number, then click **NEXT**.

9. You should receive a security code shortly after that.

   Enter the code, then select **CHECK**.

10. After the initial check is performed, click **FINISH**.

> **Note**
> You will be informed if any breaches, personally identifiable information or potential impersonation attempts are discovered during this first check.

Bitdefender Digital Identity Protection is now configured.

Reviewing your Digital Footprint, Data Breaches and possible Impersonations

After you complete the configuration, Bitdefender Digital Identity Protection performs an online check to discover potential impersonations, data breaches and personally identifiable information on the Open Web. We recommend reviewing every piece of info included in the **DIGITAL FOOTPRINT**, **DATA BREACHES** and **IMPERSONATION CHECK** tabs.

- Reviewing your Digital Footprint
- Reviewing Data Breaches
- Reviewing possible Impersonations

Improving your check-up

We use the data you provide to monitor the Surface Web and Dark Web to detect any activity that might affect your privacy or your personal brand reputation.

If you would like to add another email address or another phone number, click  , then click on **ADD EMAIL ADDRESS** or **ADD PHONE NUMBER** and follow the instructions.

3. DASHBOARD

The Dashboard aggregates information included in the **DIGITAL FOOTPRINT**, **DATA BREACHES** and **IMPERSONATION CHECK** sections.

It includes the following:

- Your exposed data and their web sources
- The average amount of exposed data for the entire community
- Your Digital Footprint evolution
- Privacy-related content
- Data Breaches
- The average number of data breaches inside the community

Digital Identity Monitor

Using only accurate information Bitdefender's system looks for new personal data exposed on the Open Web and Dark Web and scans all the major Social media platforms for any signs of an impersonation attempt.

Click on **CHECK NOW** to perform an online scan.

4. DIGITAL FOOTPRINT

Your personally identifiable information and their sources appear here. It is up to you to evaluate if having the information public on the web is a threat.

Our AI-driven monitor relies heavily on correct data to detect new threats, so please tell us if the information is accurate or inaccurate.

Once you confirm a piece of information is yours, we add it to our monitoring system and improve the chances of discovering other ones in the future.

Reviewing your Digital Footprint

To review your digital footprint:

1. Go to the **DIGITAL FOOTPRINT** tab.
2. Information that has not been verified yet will appear with the text **Verify** on the right side. Click **Verify**, then select Yes or No, depending on the case.

Note

Every piece of information confirmed is added to our monitoring algorithm, improving the results displayed by our services. Information that is dismissed will no longer be displayed. However, it will still remain available on the web.

5. DATA BREACHES

Breaches occur when hackers managed to bypass a company's security measures and obtain your personal information, to sell it on the dark web. Typically, cybercriminals target login data, personally identifiable information (PII), medical records, and banking-related details.

Any organization or service can fall victim to a data breach, but those with a large consumer base make more attractive targets. Breaches commonly include names, email addresses, usernames, passwords, postal addresses, phone numbers, social security numbers (SSN) and credit card data (number, expiration date, CVV).

Reviewing Data Breaches

To review your data breaches:

1. Go to the **DATA BREACHES** tab.
2. Under some entries, you will find a list of actions required for securing your account. After performing an action, click the box next to it in order to confirm.

   If you're not sure about how to perform a task, you can always click on the link included in the task description and you'll be redirected to a page where you'll find all the necessary steps.

   Not all breaches can be dealt with in this manner. Some of them, such as **Collection #1**, won't include steps. Instead, you will be redirected to articles available online where you can find more help.

Note

Bitdefender does not store or process personally identifiable information. Only references to potential data breaches are kept, without including sensitive data.

6. IMPERSONATION CHECK

Criminals known as “pretexters” use the art of impersonation in many ways, playing the role of a trusted individual to deceive their victims and gain access to sensitive information. The practice of “pretexting” is defined as presenting oneself as someone else to manipulate a recipient into providing sensitive data such as passwords, credit card numbers, or other confidential information.

Bitdefender Digital Identity Protection monitors 25 Social Media platforms and notifies you instantly if it finds a profile that could be an impersonation attempt.

Reviewing possible Impersonations

The IMPERSONATION CHECK tab is where all possible attempts will be displayed. For each detection, you can choose one of three possibilities:

- It is an impersonation attempt
- It is your own profile
- It is a different profile

Depeding on the choice, Bitdefender Digital Identity Protection will recommend specific steps in order to deal with the issue. Every time you complete a step, you can mark it as **Done**.

7. EDUCATION

The Education tab serves as a knowledgebase where the user can find more information on how to protect their digital identity.

Articles listed here can be sorted into several categories:

- Breaches
- Exposures
- Impersonation Check

To access the full version of an article, click on its corresponding **Read more** link.

8. EVENT HISTORY

The Event History section is the means by which we communicate constantly with our users. It represents a chronologically ordered list of events regarding the protection of your Digital Identity.

Besides newly detected threats (if any), you can return to this page for valuable advice on how to properly conduct yourself online, to increase the chances of not dealing with privacy issues.

In the Event History section, you can find the following information:

- Actions performed
- Service updates
- Data Breaches