10 security tips to help keep you safe online in 2023

BY INTIGRITI · JANUARY 10, 2023 · LAST UPDATED ON AUGUST 8, 2026

Want to read the latest version? Visit the link below:
https://www.intigriti.com/blog/news/10-security-tips-to-help-keep-you-safe-online-in-2023

It's time for your annual cyber-health check

With cyber-attacks and data breaches showing no sign of slowing, now's the perfect time for your annual cyber-health check.

Here are 10 cybersecurity tips to help you to ring in the new year:

1. Use 2FA/MFA

Security-conscious readers should already be using two-factor authentication (2FA; also known as multifactor authentication, or MFA). But did you know that SMS-based 2FA is no longer considered to be secure? An increase in so-called 'SIM-swap' attacks and other mobile hacks means SMS authentication should be ditched in favor of authenticator apps wherever possible.

1. Use a password manager

Reusing passwords is never a good idea. A password manager is a digital vault for your passwords and other sensitive login data. Depending on your requirements, there are open source solutions or enterprise-grade password managers for business use – just make sure that you never share (or forget) your master password when using password management software!

1. Keep all software up to date

Ensuring your desktop and mobile operating systems, along with any apps and software, remain up to date automatically boosts your cybersecurity defenses. In addition to new features and performance improvements, software updates often include patches for any known security vulnerabilities, meaning the latest version is always the most secure. The same applies to IoT devices, whether this is a CCTV system, voice controller, or 'smart' refrigerator.

1. Launch a VDP

Does your website make it easy for researchers to know where to report any vulnerabilities or bugs they find that impact your business? A vulnerability disclosure policy (VDP) is a way of enabling businesses to mitigate security risks by providing support for the coordinated disclosure and remediation of vulnerabilities before they're exploited by cybercriminals. VDPs tend to give guidance on how the vulnerabilities should be reported and any other 'rules of engagement' for security researchers.

1. Start a bug bounty

Bug bounty remains a hot topic in cybersecurity as more and more companies open their systems to ethical hackers as part of a layered security approach. The benefits of bug bounties are clear to see, but as with any security initiative, some care needs to be taken to develop the right program for your business. Find out how Intigriti can help.

1. **Create an incident response plan**

Even the best-laid plans can go awry, and that's why all businesses should create an incident response (IR) plan that outlines the steps that should be taken in the worst-case scenario. Encryption, too, can be a savior if an employee has their laptop lost or stolen.

1. **Use Single Sign-On**

Single sign-on (SSO) is an authentication mechanism that allows a user to log into a single service to gain access to several related yet independent systems. Many readers will be most familiar with SSO when they encounter the 'Sign in with…' button that is now found on many web applications.

Did you know that Intigriti offers its customers the option to implement Single-Sign-On to ensure their bug bounty programs remain secure? Find out more.

1. **Stay aware**

Phishing is an ongoing threat, and if anything, cybercriminals are upping their social engineering game. Stay alert to phishing emails by checking the sender's email domain. Other red flags can include bad spelling or grammar, 'urgent' requests that intend to cause panic, or unsolicited calls to send money to their account.

1. **Always lock your device**

Users are often logged into several websites or applications simultaneously during their day-to-day work life. Whether a mobile, desktop, or laptop, an unlocked device makes it trivial for an assailant to take over these accounts or perform harmful actions. For this reason, ensure you always lock your screen – even if you only leave the device unattended for a short time.

1. **Launch a Hybrid Pentest**

Intigriti's Hybrid Pentest solution brings an entirely new approach to bug bounty and security testing. Supersede traditional penetration testing, secure your assets, and be ready to counter modern-day threats by harnessing the power of the crowd. Find out more.

Keep updated with more cybersecurity tips and topical discussions on our blog.