Safer Internet Day

10 WAYS YOU ARE MAKING YOURSELF VULNERABLE ONLINE

BY NODEPOSIT365.CO.UK

IN AID OF SAFER INTERNET DAY (6TH FEBRUARY), THE EXPERTS AT NODEPOSIT365.CO.UK ARE HIGHLIGHTING TEN OF THE MOST COMMON WAYS ONLINE USERS PUT THEMSELVES AND THEIR PERSONAL DATA AT RISK.

Global cybercrime is increasing year on year, with the number of personal cyber-attacks increasing by 125% in 2021, compared to 2020, and experts expect cybercrime to worsen as fraudsters become more intelligent.

Recently, one of the largest data breaches to date could compromise billions of accounts worldwide, prompting concerns about widespread cybercrime.

Therefore, experts at NoDeposit365.co.uk believe now is the time to be extra vigilant when using the internet, from online banking and shopping to entering passwords and connecting to Wi-Fi.

Overleaf, the No Deposit Bonus Codes experts at NoDeposit365.co.uk share the ten most common ways users put themselves at risk of data breach online.

USING PUBLIC WI-FI

Using public Wi-Fi is risky without proper precautions. This is because hackers can take advantage of public Wi-Fi's lax security to spy on you and steal your personal information and passwords.

Identity theft is the biggest risk when using public Wi-Fi. If you are not using a virtual private network (VPN) to hide your information, hackers can easily pinpoint information about you.

Some hackers have specialised tools that search for passwords you have saved in your browser or typed into websites, apps, or emails while using public Wi-Fi.

Once they have this information, they can perform targeted cyberattacks and phishing emails. They can also try to find out your passwords and hack into your online personal accounts.

The information they can obtain includes your location data, your work, your marital status and detailed financial information about your bank and credit.

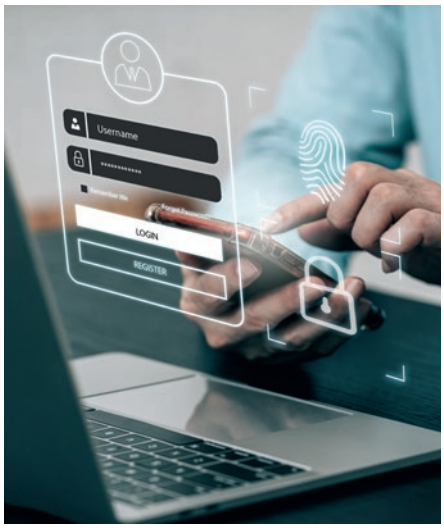
How to keep safe: If you do need to use public Wi-Fi, use a virtual private network (VPN) when connecting to any Wi-Fi hotspot (including your own). This is because a VPN connection disguises your data traffic online and protects it from external access.

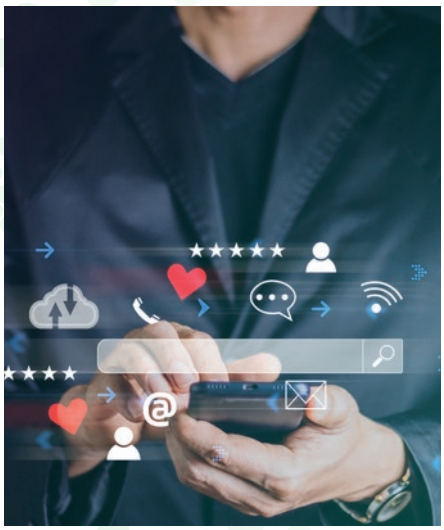
PRIVACY SETTINGS ARE NOT SO PRIVATE

Web browsers and mobile operating systems have settings to protect your privacy online for a reason.

Whilst marketing companies and hackers can both learn a lot from your browsing and social media usage, you are able to stop this using the enhanced settings available in your applications.

If a cybercriminal has their eye on you as a potential victim, any information such as full name, date of birth, home address, contact number, email address, photos or videos can help them get a step closer to hacking you.





Many things including your personal social media direct messages, GPS and photographs can be accessed easily if you are not restricting third-party access to apps such as Facebook, Twitter, Instagram, LinkedIn, TikTok etc.

When downloading an app, we will automatically accept a privacy policy without reading them. With so much data used for marketing and advertising, it is a good idea to review the privacy policies of the apps and websites you use to understand how your data is collected and analysed.

How to keep safe: Restrict third-party access in the applications you have personal data contained in. Often in the settings of these apps, or in your iPhone's application settings, there will be a "Revoke Access" button in which you can adjust the setting.

USING THE SAME PASSWORDS FOR SEVERAL ACCOUNTS

32% of internet users reuse the same password across 5 to 10 websites and apps. This is one of the most risky things you can do, as once a hacker guesses one password, they can guess several. This is where your accounts can be accessed, and personal data can be leaked or tarnished.

How to keep safe: increase the difficulty of your password. Make it long with at least 12 characters or more, use a mix of characters both upper and lower-case including symbols and numbers, and avoid using sequential numbers ("1234") or personal information that someone who knows you might guess, or that might already be online, such as your place of birth or a dog's name.

KEEPING UNUSED ACCOUNTS OPEN

Unused accounts that are still open are likely to have weaker passwords and poor data protection policies.

Therefore, if your easy-to-access account is still open, it can put you at future risk of having your current accounts hacked. This is because any remaining personal information within this account that is accessed by a cybercriminal could be used against you for further attacks.

How to keep safe: Close any old online accounts and request that your data be deleted from the relevant third-party servers.

CARELESSLY CLICKING ANY LINKS

Clicking a malicious link can expose your personal data online or infect your device with malware.

Normally, malicious links are lurking on things such as online quizzes, free offers, unsolicited adverts, spam emails etc.

Often if you are on a website on a particular topic, and then there is an advert to click to something completely different, this should raise alarm bells.

How to keep safe: When you are on a website, make sure links click through to relevant or expected topics. As for emails, it is best to avoid opening untrusted emails at all. If you are not sure whether an email is legitimate or not, go directly to the source and follow it up there.

NOT USING MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) is another layer of security that requires you to verify your identity with more than one piece of information before accessing an account.

An example of this could be using a fingerprint or facial recognition scan, after entering a password. This layer of security makes it harder for hackers to access your account, even if they have your password.

How to keep safe: Enable MFA whenever possible, especially for accounts that contain sensitive or valuable information, such as banking, social media, or email accounts. You can do this in the setting of any of your email accounts and there are some apps also dedicated to layering this security across several of your apps.

OVERSHARING ONLINE

Social media is great for sharing your whereabouts with friends and family. However, many people forget that social media sites are still a public domain and can be accessed widely.

If a cybercriminal has their eye on you as a potential victim, any information such as full name, date of birth, home address, contact number, email address, photos, or videos can help them get a step closer to hacking you.

Therefore, sharing too much personal information online can make us vulnerable to identity theft, fraud, phishing, cyberstalking, and other cybercrimes. It can also impact reputation, relationships, and opportunities in the future depending on the repercussions.

How to keep safe: Be careful about who we share our information with online and only share with people we know and trust on secure platforms that have privacy settings that we can control, as opposed to a public domain.

NOT KEEPING ANTIVIRUS SOFTWARE UP TO DATE

It is important to not neglect security and ensure you are running regular antivirus and malware protection scans.

When it comes to online shopping, having a comprehensive, up-to-date security solution not only removes the uncertainty associated with online transactions, makes online shopping safer.

How to keep safe: Your antivirus software should be set as default to check for updates at least once a day, but also check to make sure this is the case. You can run an on-the-spot scan at least once a week to check for the latest threats.

NOT HAVING A FIREWALL SET UP

A firewall does what it says on the tin - keeps something in or out.

In your case, a firewall will act as a barrier for any unauthorised intruders who may want to access your network. Firewalls monitor all incoming and outgoing traffic occurring within your device's network.

A firewall will work alongside a pre-established set of guidelines. Therefore, giving you ultimate control over monitoring your network access.

How to keep safe: You can configure a firewall to flag any unauthorised entry and block it too.

You can do this in five steps.

1. Secure your firewall.
2. Architect your firewall zones and IP addresses.
3. Configure access control lists.
4. Configure your other firewall services and logging.
5. Test your firewall configuration.

BEING UNEDUCATED

If you are going to use the Internet, you should take some time to research trends and look up any ongoing news regarding data breaches, security status etc.

Particularly if you work remotely or own your own business with remote workers, putting secure, robust systems in place to keep you and your business network educated and safe is extremely important.

You should ensure every member of staff is security trained and knows exactly what to look out for when cyber threats or malware occur.

How to keep safe: Participate in or offer regular online safety training. Also, ensure all important data is backed up on a separate storage drive and be prepared if your personal data is hacked.

www.nodeposit365.co.uk