Safeguard your digital presence from Hackers

Beware and Be-aware about how to safeguard your digital presence from hackers


Shitesh Sachan

DELHI, NEW DELHI, INDIA, March 5, 2021 /EINPresswire.com/ -- Avoid public Wi-Fi

This may sound obvious, but you would be shocked how many people use public Wi-Fi to search their bank balances or make credit card transactions. Wi-Fi networks that don't need a password and are commonly used have no authentication features. As a result, they're prime targets for cybercriminals. It's preferable to do so over a safe network.

Switch- it of anything you don’t need

Hackers may access your passwords, location, or link by exploiting certain features on your phone. So, rather than leaving your Bluetooth, GPS, wireless link, or geo-tracking on all the time, just use them when you need them. as an example Switch off Bluetooth while you're not using it. Leaving your Bluetooth turned on but dormant allows hackers to gain access to your phone.

> 100% security is not a myth, Just we need to understand that it's everyone's responsibility.”
>
> *Shitesh Sachan*

Similarly Autocomplete is a another feature that guesses what you're typing and fills in the blanks with the name, expression, or other detail. Though useful, this tool effectively gives hackers your email address, postal address, phone number, and other personal details. Switch it off.

Trusted-Apps

Just download applications from reputable sites with a clear track record. Prefer to use only those apps available on Google Play Store or Apple Store.

Use a password - lock code or encryption--
The most effective way to avoid network intrusions is to use complex passwords. A intruder would have a tougher time breaking into your system if your passwords are complex. Using no recognizable words or combinations that may be linked to you, such as birthdays or other personal knowledge. Don't use the same password twice. Make sure the passwords are at least eight characters long, have numbers or other characters, and never use the auto-complete option for passwords. To secure your personal information, enable the storage encryption option on your phone and set your screen to timeout after five minutes or less. Even if cybercriminals gain access to your network and files, encryption will prevent them from gaining access to all of your data. 0000,1111,0123,1234 are simple unlock codes to recall, but they're still simple to guess. Instead, use a six-digit passcode that is created at random.

Be careful about links, attachments and spams

Do not click or open the attachment if you are unsure about the source. Always beware of emails from unknown senders, and never click on links or open attachments in them. Spam scanners in email inboxes have gotten pretty good at capturing the most obvious spam.

However, more advanced phishing emails that imitate your colleagues, employees, and trustworthy companies (such as your bank) are becoming more popular, so be on the lookout for something that looks or sounds suspicious.

Remove Browsing history

If your mobile device is hacked or destroyed, make sure your data is secure. After a certain number of unsuccessful log-in attempts, you can configure your smartphone to lock itself. A surfing history exists in your smartphone web browser as well. Clear it often, like cookies and cached data, to send hackers as little information as possible if they do manage to gain access to your phone.

Use 2FA

Passwords are the first line of defense against computer hacks, so adding a second layer of protection increases security. Many websites allow you to enable two-factor authentication, which increases protection by requiring you to log in with both your password and a numerical code sent to your phone or email address.

Backup of digital devices

If your company isn't backing up its hard drive yet, you should start doing so right away. Backing up your data is important in the event that hackers succeed in breaking into your device and destroying it.

Keep your software updated

Often keep the operating systems up to date by installing new upgrades. Most updates provide security patches that prevent hackers from gaining access to and manipulating your information. Similarly do for your smartphone OS, Apps and other related software's. Check to see if your smartphones and software are up to date, and get rid of those apps you aren't using.
Web browsers are becoming more advanced, particularly in terms of privacy and protection. In addition to downloading all latest patches, make sure to refresh the browser's security settings. You may use your browser, for example, to prohibit websites from monitoring your activities, thus increasing your online privacy. Alternatively, you should use one of the private web browsers.

Make sure firewall is active and enable

Before you go online, make sure the firewall is turned on. Firewalls protect the company's network from unwanted entry and notify you of any attack attempts.

Shitesh Sachan Founder & CEO
Detox Technologies
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
