INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on Internet

WATCH OUT FOR THE COVID-19 VACCINE REGISTRATION SCAM

More than a year since the World Health Organization (WHO) declared COVID-19 a pandemic, the news that the COVID-19 vaccine is around the corner has made many people impatient. But excitement mixed with uncertainty can leave one vulnerable.

A new Android malware is making rounds on the Internet, luring people in the name of free registration for the Covid-19 vaccine. A fake SMS is in circulation that carries a link that installs the malicious app on android devices. When the user gives permission to share contacts, the malware spreads itself by sending SMS to the victim's contact.

The malicious application circulates with different names such as: Covid-19.apk, Vaci_Regis.apk, MyVaccin_v2.apk, Cov-Regis.apk, Vccin-Apply.apk

OTHER STORIES INSIDE THIS ISSUE:

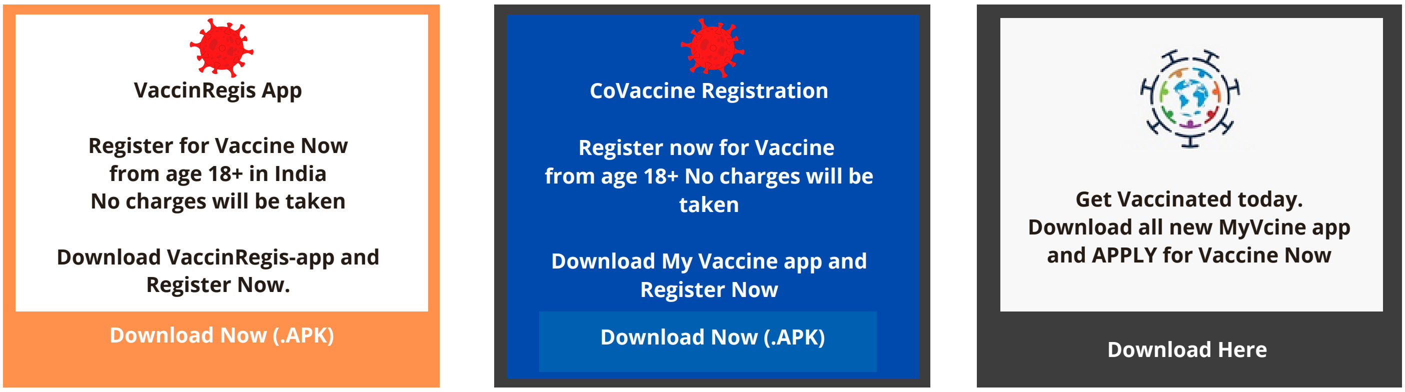
https://twitter.com/IndiaFutureFou2

https://www.facebook.com/indiafuturefoundation5

https://www.instagram.com/india_futurefoundation/

https://www.linkedin.com/company/india-future-foundation/

Snapshots of the malicious apps



VaccinRegis App

Register for Vaccine Now
from age 18+ in India
No charges will be taken

Download VaccinRegis-app and
Register Now.

Download Now (.APK)

CoVaccine Registration

Register now for Vaccine
from age 18+ No charges will be
taken

Download My Vaccine app and
Register Now

Download Now (.APK)

Get Vaccinated today.
Download all new MyVcine app
and APPLY for Vaccine Now

Download Here

Best practices:

- Always use the official application for covid vaccine registration – CoWIN portal.
- Download android applications from Play Store.
- Beware before opening or clicking any links.
- Do not enable installation of apps from "Untrusted Sources" in the mobile device
- Consider using safe browsing tools and antivirus
- Do not share personal and sensitive information to unknown and unfamiliar websites and mobile applications
- Beware before downloading or opening unknown documents

Source: CERT-In

SAFEGUARD YOURSELF FROM PHISHING ATTACKS

Malicious actors and cyber scammers always find new ways to scam people, like taking advantage of the pandemic by sending fraudulent and unsolicited emails related to the pandemic that attempt to trick the user into clicking malicious links. Phishing attacks are continuously on the rise. Here are some of the common ways of phishing that you should be aware of:

Email Phishing

The malicious actors register fake domains or mimics a genuine organization and send mass emails to many. To detect email phishing attacks, one can check the domain name in the sender's address, look for strange or unexpected attachments. In addition, malicious actors create a sense of urgency in the email to force people into action.

****
Please enter your password here
Fluffy2020
Please send me your information real quick:
Please enter your credit card number:

Vishing

Vishing is carried out when a malicious attacker calls and acts as an authentic individual or organization to deceive people. In this type of attack, attackers try to create some sort of urgency. Beware of this type of attack and look for suspicious behaviour during a call.

Spear Phishing

Spear phishing is targeted and personalized to specific individuals. Malicious actors have some information about their targets like name, job title, and other personal information.

Email security solutions can protect against such spear phishing attacks.

CEO fraud Phishing

In CEO fraud phishing, cyber criminals spoof the CEO's email address and trick employees to transfer money or gain sensitive information. The attacker either spoofs the mail if there is no email security in place or tries to use a similar domain name and hopes that the recipient doesn't notice the incorrect address.

Using anti-phishing software and creating awareness among employees about common techniques can prevent such types of attacks.

SECURELY USING MOBILE APPLICATIONS

Mobile phones have become one of the primary technology that people use both personally and professionally. These devices offer a plethora of applications that enable people to be more productive, communicate, and so much more. Here are some of the steps one can take to securely use and make the most of today's mobile apps.

Cybercriminals and malicious actors have mastered their skills at creating and distributing legitimate-looking malicious applications. Once these malicious apps are installed and given permissions, it can lead to a complete takeover of the mobile device and data. Therefore, one should always install apps from trusted sources only.

For Apple devices, only download mobile apps from the Apple App Store. Apple does a security check of all mobile apps before making them available to the Apple App Store. While it is tough to catch all malicious apps, this managed environment dramatically reduces the risk of downloading malicious apps. Moreover, Apple is quick to remove any app that it believes to be malicious from its app store.

For Android devices, only download mobile apps from Google Play, which Google maintains. Like Apple, Google does a security check of all apps before making them available to users. The difference with Android devices is that you can also enable certain options that allow you to download mobile apps from other sources. This option makes it easy for cybercriminals to trick users into downloading apps and infect the mobile device.

Another good cyber hygiene to keep in mind is the permissions for the apps. Make sure to enable permissions that are actually required and not enabling all permissions. Excessive permission can lead to sharing of data with the creators of the application. The creators can utilize the data in the ways they seem fit or even sell the data to others. Deny the permissions that you think are not required and grant permissions only when it's actively being used, or look around for another app that meets your requirements and doesn't ask for excess permission for the app's functioning.

Updating mobile apps is another crucial factor in being safe on the internet. Cybercriminals are constantly searching for and finding new vulnerabilities in apps and developing ways to exploit these vulnerabilities. The app's developers release security updates to fix these vulnerabilities. Most devices allow you to configure automatic updates for the apps. One can enable such a setting in the app store.

WHY COLONIAL PIPELINE PAID $4.3 BILLION TO HACKERS?

On 7th May 2021, Colonial Pipeline that carries gasoline and jet fuel, suffered a ransomware cyberattack. The entire cybersecurity community is riveted by the Colonial Pipeline ransomware attack. It is one of the most notable attacks on critical infrastructure in the past few years and impacted multiple industries in the U.S. DarkSide, the Eastern European-based hacking group, is believed to be behind the attack. Later on 10th May 2021, the FBI confirmed that the Darkside group is responsible for the ransomware attack. The group used Ransomware as a Service (RaaS) against Colonial Pipeline. The ransomware is carefully prepared and deployed and uses a combination of techniques to extort its victims successfully. As a result, the pipeline went down for several days and caused panic-buying among the citizens.

The Colonial Pipeline hackers entered the company's IT systems through virtual private network (VPN) using an old login credential.

This system was not protected by basic industry-standard security protocols. From there, the hackers locked up important company information and demanded a ransom.

Colonial officials realised that shutting down the pipeline would have major ramifications as they hurried to respond to the rupture. But they couldn't run the risk that hackers might "move laterally" through the company's infrastructure and cause lasting damage. If hackers had done so, the time it took for gasoline delivery to return to normal may have been extended.

So managers shut down the pipeline and engaged with the hackers, and paid them 75 bitcoin in ransom, worth $4.3 million at the time, according to the FBI. Authorities since then recovered more than half the ransom — about $2.3 million. Colonial submitted an insurance claim to cover its costs.

MYSTERY MALWARE STEALS 26 MILLION PASSWORDS

Malicious actors use the dark web as a marketplace to sell stolen data, credentials, credit card information, and much more. This information is brought and sold on an industrial scale. On 9th June 2021, researchers highlighted a breach that contained **1.2 terabytes** of data. A hacker group accidentally revealed the location of the stolen database.

The stolen database contains 1.2 TB of files, cookies, autofill data, payment information, and credentials obtained from 3.2 million Windows-based computers. The analysis of the data shows the data is extracted between 2018 and 2020. The database includes 2 billion cookies. The analysis of the cookies' data reveals that over 400 million, or 22%, of those cookies are still valid.

The database contained **26 million login credentials** with **1.1 million unique email addresses**. Researchers believe that the malware escaped with 6 million files it grabbed from Desktop and Downloads folders. Three million text files, 900,00 image files, and 600,000+ Word files made up the bulk of the stolen database, but it also contained over 1,000 types of different files.

The malware spreads via pirated software and games like pirated Adobe Photoshop, Windows cracking tools, and pirated games. Moreover, the malware photographs the user if the computer has webcam.

ROCKYOU2021: LARGEST PASSWORD COMPILATION

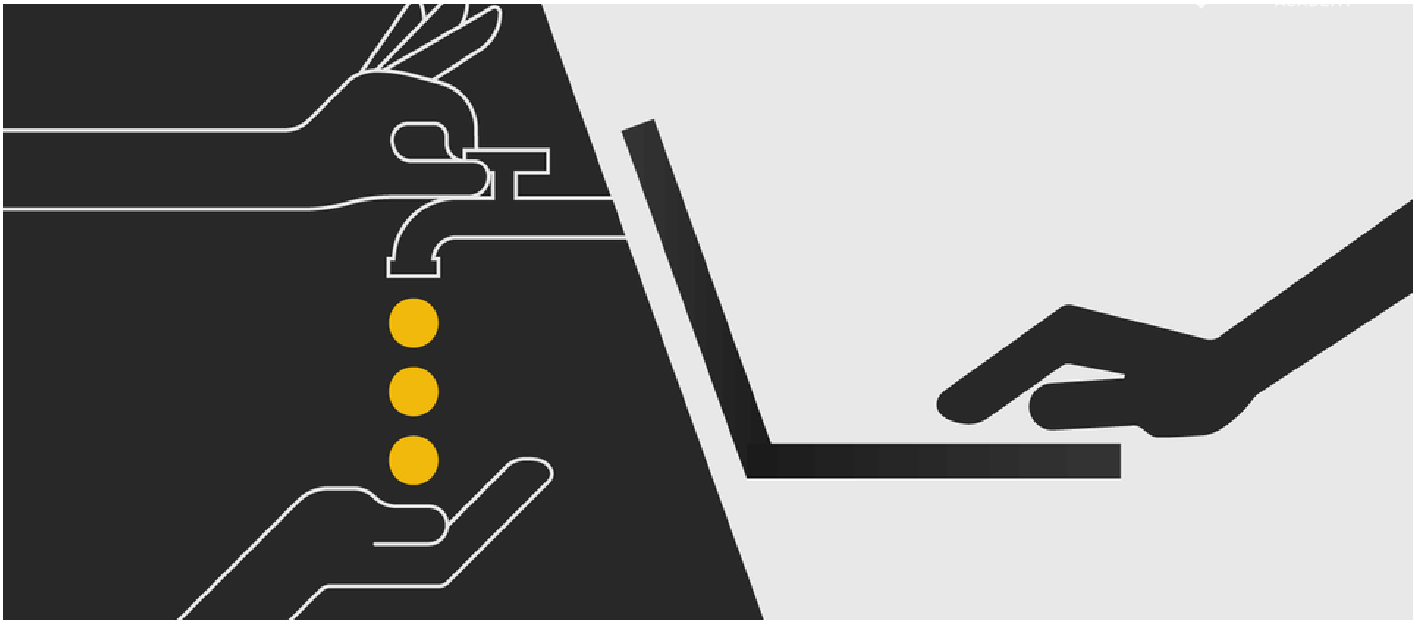
princess 1234567 rockyou
babygirl monkey lovely jessica
qwerty 111111 iloveu
password1 soccer anthony friends
princess 1234567 rockyou
daniel babygirl monkey lovely jessica
iloveyou qwerty 111111 iloveu michelle
password1 soccer anthony friends
princess rockyou 12345678 angel
babygirl monkey lovely jessica 654321
qwerty 111111 iloveu 000000 michelle
soccer anthony friends butterfly
1234567 rockyou 12345678 angel
lovely jessica 654321 michael
michelle 12345 tigger

In 2009, threat actors hacked the RockYou servers and extracting over 32 million plaintext passwords by exploiting a SQL injection vulnerability. In June 2021, a new password compilation is leaked on a forum that is 262 times the 2009's rockyou compilation. The compilation consists of **8.4 billion passwords** in a 100GB text file and is dubbed "Rockyou2021". The compilation contains past credentials breaches that contain passwords ranging from 6 to 20 characters. Threat actors can use the compilation to execute attacks like dictionary attacks or password spraying against users and organizations.

CRYPTOJACKERS PREY ON THE UNINFORMED

Cryptocurrency transformed the financial world in novel ways, but it is not all positive. The crypto world now introduces new threats and risks like cryptojacking. Like the computers brought new forms of scamming, the crypto world presented us with cryptojacking scams. Cryptojacking, like other scams, preys on the uninformed as well as some knowledgeable people can fall prey to such scams.

Cryptojacking perpetrated when a malicious actor uses someone else's computer without his or her consent to mine cryptocurrency. Malicious actors through the use of some techniques install the malware in the victim's computer. This malware runs in the background and uses the victim's computational power and resources to mine cryptocurrency. The malware can cause the victim's computer to run slower or lag. The malware is difficult to detect and easy to deploy and so it is becoming a popular choice of attack vector amongst cybercriminals.

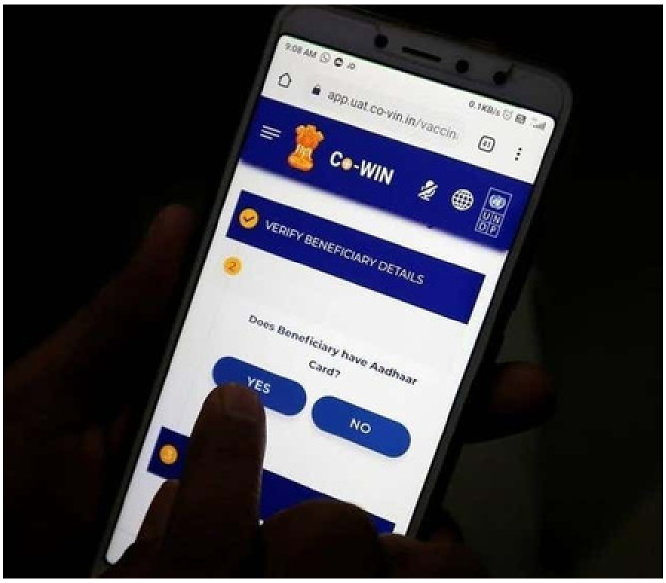


Hackers inject malicious Javascript code into an ad or website. The script auto-executes in the victim's browser when they visit the site or get the ad pop-up. This attack approach only infects the victim's browser and runs as long as the victim uses the browser.

Another approach by which cryptojacking is carried out is by sending emails with malicious URLs to victims. These carefully crafted emails appear authentic and provide the victim with some reason to click the link, which executes malicious code and installs crypto mining scripts on the victim’s machine. With this approach, the victim’s entire PC gets infected with the cryptomining script. Awareness is a crucial aspect to prevent cryptojacking. Employees need to understand and detect cryptojacking. The use of anti-crypto mining extensions like minerBlock and No Coin in the browser can help block crypto miners.

COWIN HACK IS BASELESS: GOVERNMENT

A website called Data Leak Market claims that the data of vaccinated Indians is leaked on the dark web and is available for sale. The CoWIN platform stores citizens' names, ages, gender, and mobile number. The website Data Leak Market claims that a database is available for sale for $800 on the dark web. The leaked data includes the name, Aadhar number, location, and phone number of citizens who registered through the CoWIN platform. The website claims that it is a reseller and not the original leaker of data. However, the health ministry and security researcher soon refuted the claims of the website.


app.uat.co-win.in/vaccin
Co-WIN
VERIFY BENEFICIARY DETAILS
Does Beneficiary have Aadhaar Card?
YES
NO

RS Sharma, who heads the CoWIN platform said, "Our attention has been drawn towards the news circulating on social media about the alleged hacking of Co-WIN system. In this connection, we wish to state that Co-WIN stores all the vaccination data in a safe and secure digital environment. No Co-WIN data is shared with any entity outside the Co-WIN environment. The data is claimed as having been leaked such as geo-location of beneficiaries is not even collected at Co-WIN. The news prima facie appears to be fake. However, we have asked the Computer Emergency Response Team of MeitY to investigate the issue." Researchers refuted the claims of the CoWIN Portal Hack and called the act as a bitcoin scam.

Source: https://www.indiatoday.in/technology/news/story/fake-website-claims-cowin-data-of-150-million-leaked-security-researchers-call-it-a-bitcoin-scam-1813451-2021-06-11

GOOGLE RUSHES TO FIX CHROME ZERO-DAY VULNERABILITY

Google released an update to fix a zero-day vulnerability in the Chrome browser. Google fixed the vulnerability by releasing Chrome 91.0.4472.114 for Windows, Mac, and Linux on 17th July 2021. Beyond the high-severity zero-day, the new release fixes other security loopholes as well.

The company announced in its blog that it is aware that an exploit exists for this zero-day. An anonymous researcher reported the vulnerability on 15th July 2021. The zero-day is exploited by the "use after free" bug in the WebGL (Web Graphics Library) JavaScript API used by the Chrome web browsers to render interactive 2D and 3D graphics without using plug-ins. Successful exploitation can lead to arbitrary code execution on the unpatched Chrome versions.

Source: https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop_17.html

G7 SUMMIT TURNS SPOTLIGHT ON CYBERCRIME AND RANSOMWARE

In the 47th G7 Summit held on 11-13 June 2021, the world leaders highlighted the increasing cyberattack menace and make it a priority to counter ransomware attacks. The increasing sophistication, frequency, and persistence of these attacks disrupted the world in the pandemic. With high-profile attacks like the Colonial Pipeline ransomware attack and JBS ransomware attack, where the companies paid the ransom in bitcoin, the G7 leaders vowed to combine forces to combat the cyber attacks.

The Summit's final communique called on Russia "to account those within its borders who conduct ransomware attacks, abuse virtual currency to launder ransoms, and other cybercrimes."

APPLE ISSUES URGENT PATCHES FOR 2 ZERO-DAY VULNERABILITIES

Apple shipped out-of-band security updates to patch two zero-day vulnerabilities in iOS 12.5.3. The company states that threat actors may have previously exploited the zero-day vulnerabilities. The CVE IDs for the two vulnerabilities are CVE-2021-30761 and CVE-2021-30762. The Common Vulnerabilities and Exposures (CVE) is a reference method for publicly disclosed vulnerabilities, and each vulnerability has a CVE ID.

The bugs are found in the Webkit browser engine that allows arbitrary remote code execution on vulnerable devices. This is the 9th zero-day vulnerability related to Webkit and the 12th zero-days this year. The CVE-2021-30761 vulnerability exploited a memory corruption issue to gain arbitrary remote code execution. The CVE-2021-30762 vulnerability is a use-after-free issue that also leads to arbitrary code execution. The impacted devices include older apple devices such as iPhone 5s, iPhone 6, iPhone 6 Plus, iPad Air, iPad mini 2, iPad mini 3, and iPod touch (6th generation). The two zero-day vulnerabilities are reported to Apple by anonymous researchers.

INDIA FUTURE FOUNDATION

India Future Foundation

Phone: +91-1244045954, +91-9312580816
Email: helpline@indiafuturefoundation.com
BSMT, Building no. 2731 EP, Sector 57, Golf Course Ext. Road, Gurugram,
Haryana, India – 122003
www.indiafuturefoundation.com