kindred

Security Newsletter

22 February 2021

Subscribe to this newsletter

Beware of COVID-19 vaccine scams and misinformation

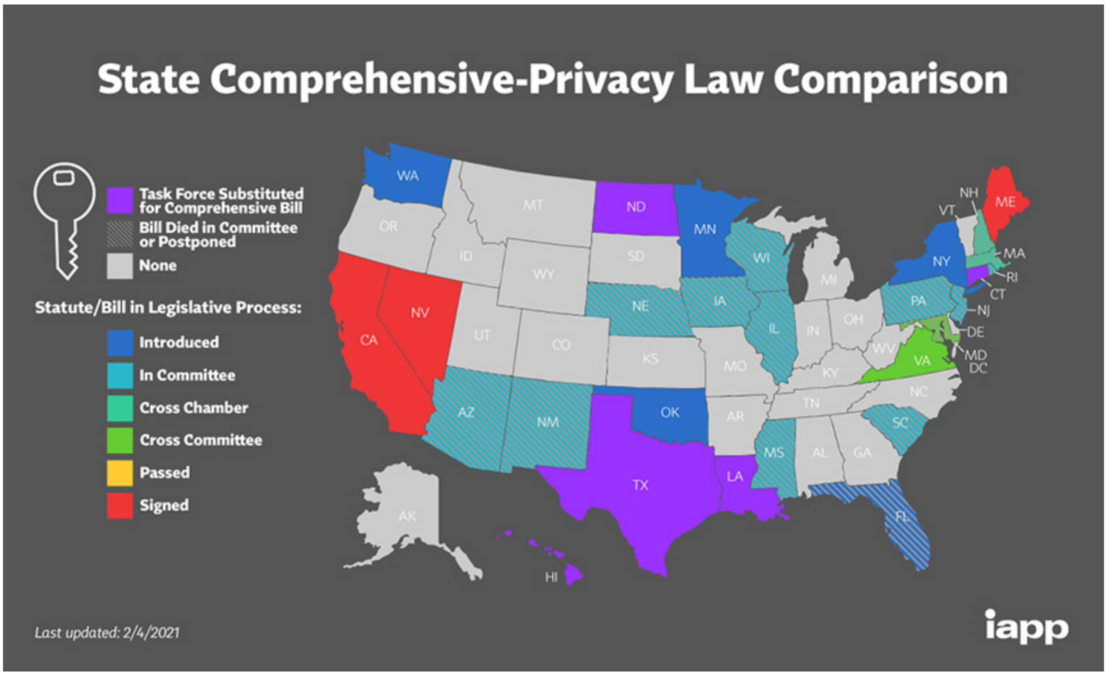
The rollouts of COVID-19 vaccines are steadily gaining speed, sparking hope that we may see the end of the pandemic and return to normal life sooner rather than later. This, however, has not escaped the notice of enterprising scammers who would like to cash in on the vaccine distribution effort by using fake offers and spewing out fraudulent emails.

One common tactic involves offering various ways people could capitalize on the pandemic and vaccine rollout. These scams typically focus either on the COVID-19 vaccines themselves, or on the tech used to manufacture or store them. Another frequent tactic relies on posing as a health authority that is directly involved in battling the pandemic. The World Health Organization (WHO) has been among the most impersonated authorities in various COVID-19-related scam campaigns, with scammers – masquerading as WHO representatives and employees – trying to disseminate fake apps or pretending to offer important information.

These are just some of the examples of vaccine-themed scams that you might stumble upon and you can be sure that enterprising crooks will be doubling down on their efforts as the vaccine rollout continues. Also, given the rapid increase in new coronavirus variants, it would not be surprising to see that pop up in COVID-19-themed scams. One of the easiest ways you can stay safe is by using a reputable security solution that includes a spam filter. However, if you do receive an unsolicited email from someone you don't know: always be extra vigilant and scrutinize it for telltale signs of a scam, including those described above.

Read More on WeLiveSecurity

Privacy Legislation Progresses in 5 More States



State Comprehensive-Privacy Law Comparison

Last updated: 2/4/2021

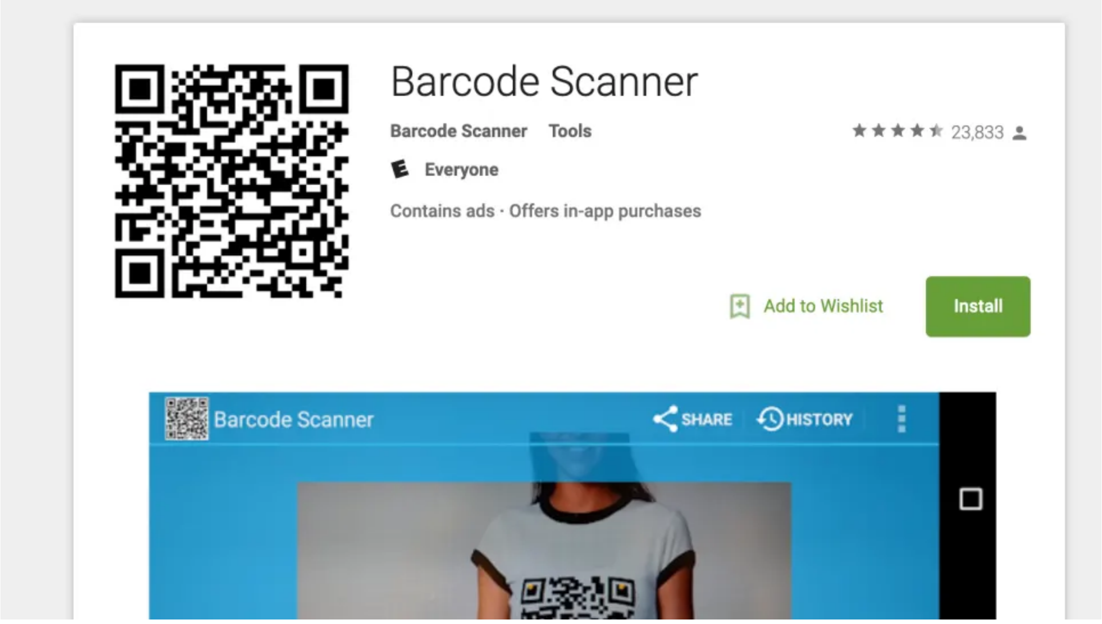
Five states are making progress this year toward passing privacy legislation along the lines of California's Consumer Privacy Act, according to the International Association of Privacy Professionals.

If Virginia, Minnesota, New York, Washington and Oklahoma succeed in enacting new privacy laws this year, the total number of states with privacy regulations would go up to eight. Previously, Maine and Nevada, in addition to California, each enacted legislation. Ten other states introduced privacy legislation last year.

The majority of bills being considered at the state level are modeled on the CCPA and the recently instituted California Privacy Rights Act. Full enforcement of the CCPA began in July 2020 (see: It's Official: CCPA Enforcement Begins). Washington's pending legislation has also played an influential role.

Read More on BankInfoSecurity

Barcode-Scanning App for Android Pushed Malware Onto Millions of Phones



A popular app has been removed from Google Play after it was discovered to have delivered trojanized malware onto millions of users' phones via an update. Until recently, Barcode Scanner was a straightforward application that provided users with a basic QR code reader and barcode generator, useful for things like making purchases and redeeming discounts. The app, which has been around since at least 2017, is owned by developer Lavabird Ldt., and claims to have over 10 million downloads, the Wayback Machine shows.

However, a rash of malicious activity was recently traced back to the app. Users began noticing something weird going on with their phones: their default browsers kept getting hijacked and redirected to random advertisements, seemingly out of nowhere. For a number of people, it wasn't clear what was causing the disruptions—as many hadn't recently downloaded any apps. After enough peeved victims wrote about their experiences on a web forum, one user ultimately pointed the finger at Barcode. Researchers with Malwarebytes have verified the scanner is the culprit, releasing a new report that shows it delivered the ad-producing malware onto users' phones, probably via a December update. The update spoiled the previously benign app—taking it from "an innocent scanner to full on malware," researchers write.

Please note that the latest smartphones with iOS 13 and Android 9 and above are equipped with an advanced QR Code readers in the built-in camera app, downloading a third-party app is no longer required.

Read More on Gizmodo

Original report from Malwarebytes

More #News

- Losses to romance scams reached a record $304 million in 2020
- Copycats imitate novel supply chain attack that hit tech giants
- Apple will proxy Safe Browsing requests to hide iOS users' IP from Google
- Egregor ransomware affiliates arrested by Ukrainian, French police
- 3 North Koreans Indicted for Conspiring to Steal $1.3 Billion
- Turning the page on Solorigate and opening the next chapter for the security community
- First Malware Designed for Apple M1 Chip Discovered in the Wild
- 6 strategies to reduce cybersecurity alert fatigue in your SOC
- Microsoft's Power BI gets new tools to prevent leakage of confidential data
- Dutch police post 'friendly' warnings on hacking forums
- Introducing DAIC: A Suggested System for Preventing BEC Fraud
- Record–high number of vulnerabilities reported in 2020
- Unpatched ShareIT Android App Flaw Could Let Hackers Inject Malware

#Breach Log

- Yandex: Insider Caused Breach Affecting 5,000 Customers
- CD Projekt's stolen source code allegedly sold by ransomware gang

#Patch Time!

- Apple Patches Flaw in macOS Big Sur Upgrade
- Siemens Patches 21 Vulnerabilities in 2 Tools
- Jira Server for Slack Security Advisory
- QNAP patches critical vulnerability in Surveillance Station NAS app
- Malvertiser abused WebKit zero-day to redirect iOS & macOS users to shady sites
- Microsoft Patches Privilege Escalation Vulnerability in Microsoft Defender

#Tech and #Tools

- Python wheel-jacking in supply chain attacks
- Hidden in plain sight: mitigating the dangers of browser extensions
- ICS Vulnerability monitoring
- Web Application Security Checklist
- Threat Actors Now Target Docker via Container Escape Features
- Finding More IDORs – Tips And Tricks
- Masslogger campaigns exfiltrates user credentials
- Breaking Trust: Shades of Crisis Across an Insecure Software Supply Chain
- new Azure AD roles to minimize the need for Azure Global Administrator
- Avoiding npm substitution attacks
- NTLM Relaying 101

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us