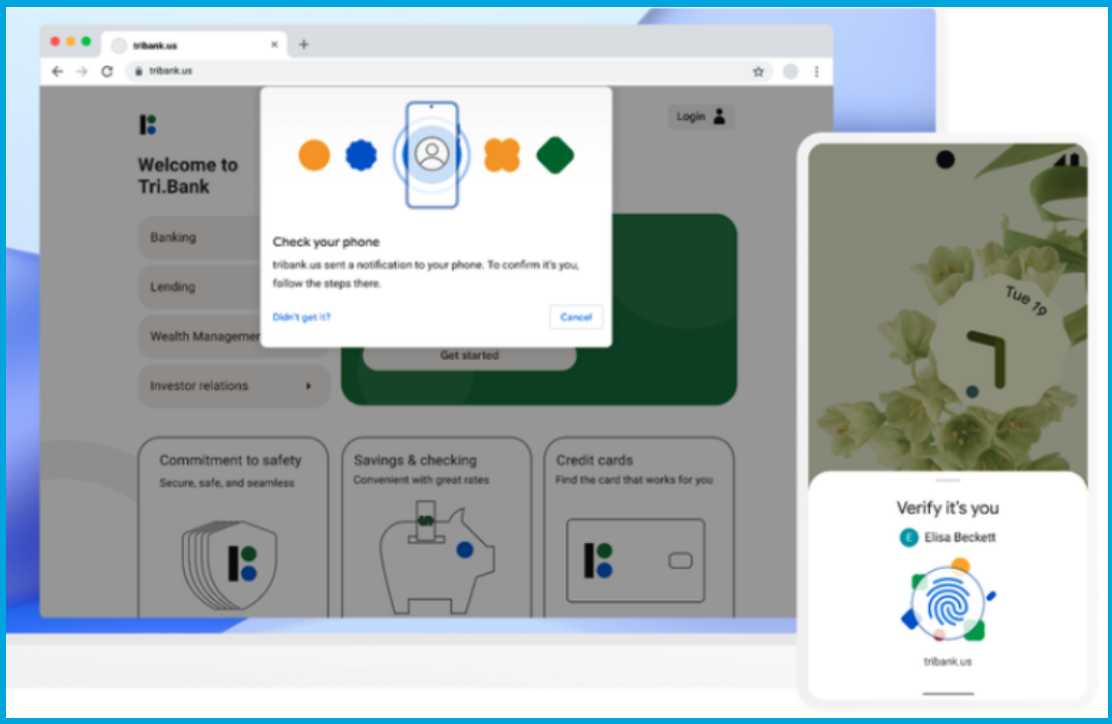
kindred

Security Newsletter

9 May 2022

Subscribe to this newsletter

Your Phone May Soon Replace Many of Your Passwords



Apple, Google and Microsoft announced this week they will soon support an approach to authentication that avoids passwords altogether, and instead requires users to merely unlock their smartphones to sign in to websites or online services. Experts say the changes should help defeat many types of phishing attacks and ease the overall password burden on Internet users, but caution that a true passwordless future may still be years away for most websites.

The tech giants are part of an industry-led effort to replace passwords, which are easily forgotten, frequently stolen by malware and phishing schemes, or leaked and sold online in the wake of corporate data breaches.

Apple, Google and Microsoft are some of the more active contributors to a passwordless sign-in standard crafted by the FIDO (“Fast Identity Online”) Alliance and the World Wide Web Consortium (W3C), groups that have been working with hundreds of tech companies over the past decade to develop a new login standard that works the same way across multiple browsers and operating systems.

Read More on Krebs on Security

More #News

- US offers $15 million reward for info on the Conti ransomware gang
- White House: Prepare for cryptography-cracking quantum computers
- FBI says business email compromise is a $43 billion scam
- Mitsubishi Electric faked safety and quality control tests for decades
- U.S. Sanctions Cryptocurrency Mixer Blender for Helping North Korea Launder Millions

#Breach Log

- Lincoln College to close after 157 years due ransomware attack
- Costa Rica declares national emergency after Conti ransomware attacks
- Ferrari subdomain hijacked to push fake Ferrari NFT collection
- US agricultural machinery maker AGCO hit by ransomware attack
- Heroku admits to customer database hack after OAuth token theft
- Car rental giant Sixt facing disruptions due to a cyberattack

#Patch Time!

- Google Releases Android Update to Patch Actively Exploited Vulnerability
- Hackers exploiting critical F5 BIG-IP bug, public exploits released
- Cisco Patches Critical VM Escape in NFV Infrastructure Software
- Check your gems: RubyGems fixes unauthorized package takeover bug
- QNAP fixes critical QVR remote command execution vulnerability
- QNAP Releases Firmware Patches for 9 New Flaws Affecting NAS Devices

#Tech and #Tools

- Years Old Vulnerabilities in Avast And AVG Put Millions At Risk
- North Korea's Lazarus: their initial access trade-craft using social media and social engineering
- Cloudflare Pages, part 1: The fellowship of the secret
- Hacking a Bank by Finding a 0day in DotCMS
- The Cloudflare Bug Bounty program and Cloudflare Pages
- Zyxel firmware extraction and password analysis

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

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering more than 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 2,000 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

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