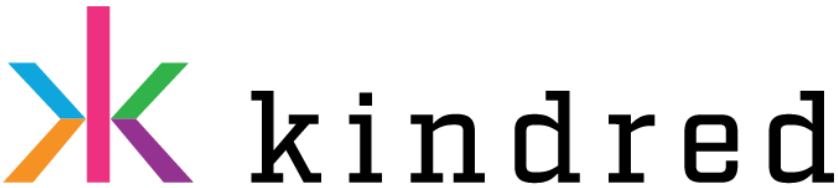



# Security Newsletter

25 March 2019

Subscribe to this newsletter

# Facebook Mistakenly Stored Millions of Users' Passwords in Plaintext

Facebook is again at the center of a new privacy controversy after revealing today that its platform mistakenly kept a copy of passwords for "hundreds of millions" users in plaintext. What's more? Not just Facebook, Instagram users are also affected by the latest security incident. So, if you are one of the affected users, your Facebook or Instagram password was readable to some of the Facebook engineers who have internal access to the servers and the database.

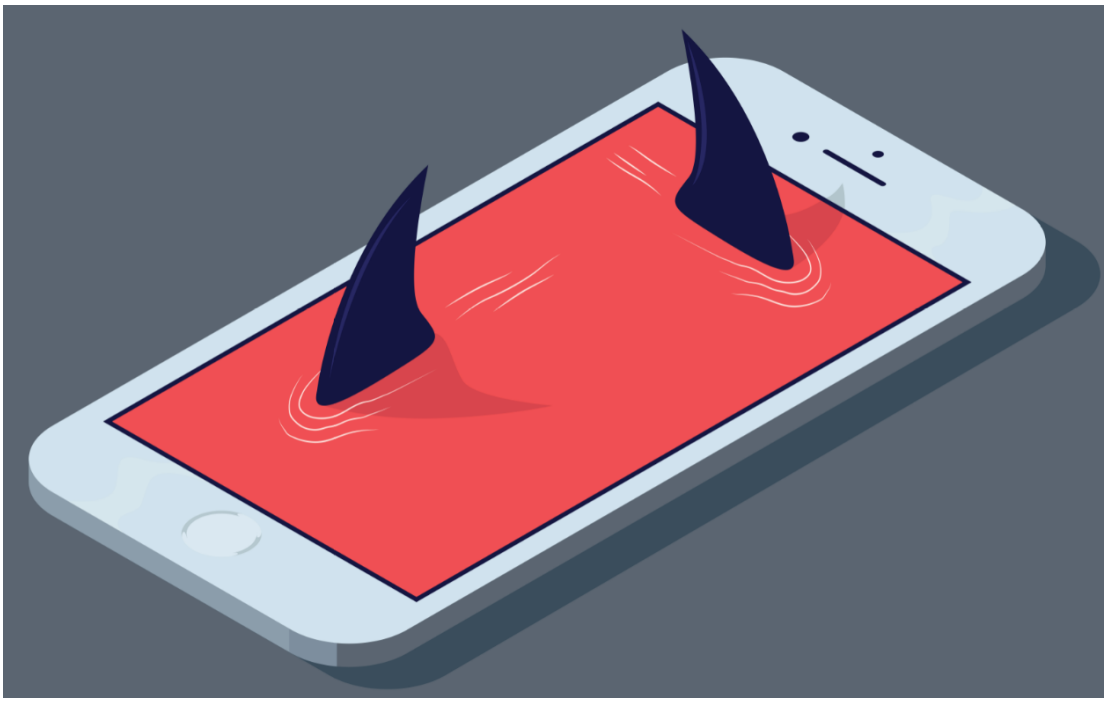
However, Facebook is not alone that exposed hundreds of millions of its users' passwords in plain text. Twitter last year also addressed a similar security incident that unintentionally exposed passwords for its 330 million users in readable text on its internal computer system.

Facebook has now fixed this issue and recommended users to change their Facebook and Instagram passwords immediately.

Read More on TheHackerNews

Official Statement from Facebook

# Why Phone Numbers Stink As Identity Proof



Phone numbers stink for security and authentication. They stink because most of us have so much invested in these digits that they've become de facto identities. At the same time, when you lose control over a phone number — maybe it's hijacked by fraudsters, you got separated or divorced, or you were way late on your phone bill payments — whoever inherits that number can then be you in a lot of places online.

How exactly did we get to the point where a single, semi-public and occasionally transient data point like a phone number can unlock access to such a large part of our online experience? KrebsOnSecurity spoke about this at length with Allison Nixon, director of security research at New York City-based cyber intelligence firm Flashpoint.

Read More on KrebsOnSecurity

## More #News

- Over 100,000 GitHub repos have leaked API or cryptographic keys
- Flaw in NSA's GHIDRA leads to remote code execution attacks
- The security implications of serverless cloud computing
- New MageCart Attacks Target Bedding Retailers My Pillow and Amerisleep
- Microsoft Brings Defender Security Tools to Mac
- Elsevier exposes users emails and passwords online
- Vulnerability in Android Instant Apps can be used to steal history, authentication tokens
- Mirai Variant Adds Dozen New Exploits to Target Enterprise IoT Devices
- Zero-day in WordPress SMTP plugin abused by two hacker groups
- Insecure Database Exposes 800,000 Singapore Blood Donors
- Researcher finds new way to sniff Windows BitLocker encryption keys
- Google Open Sources Sandboxed API

- Windows Hello Support Added to Firefox 66
- Spectrum for UDP: DDoS protection and firewalling for unreliable protocols
- What is malvertising? And how to protect against it
- Monsters in the Middleboxes: Introducing Two New Tools for Detecting HTTPS Interception
- Unsecure Fax Server Leaked Patient Data
- Microsoft releases Application Guard extension for Chrome and Firefox
- 257K Legal Documents Leaked By Unprotected Elasticsearch Server
- Over 100 Exploits Found for 19-Year Old WinRAR RCE Bug
- Uncovering the Data Security Triad
- Google Photos Bug Exposed the Location & Time of Your Pictures
- Google researcher discovers new type of Windows security weakness
- Sacked IT guy annihilates 23 of his ex-employer's AWS servers
- 2 Million Emails of 350K+ Clients Possibly Exposed in Oregon DHS Data Breach

## #Patch Time!

- Cisco Fixes High-Severity Vulnerabilities in IP Phone 77800, 8800
- PuTTY Releases Important Software Update to Patch 8 High-Severity Flaws
- Libssh Releases Update to Patch 9 New Security Vulnerabilities
- Facebook Pays Big Bounty for DoS Flaw in Fizz TLS Library
- Flaw in popular PDF creation library enabled remote code execution
- KB4493132 Update Notifies Windows 7 Users of End of Support Date
- Intel releases patches for code execution vulnerabilities
- WordPress 5.1.1 patches dangerous XSS vulnerability
- Critical Flaw in Swiss Internet Voting System

## #Tech and #Tools

- Java Serialization: A Practical Exploitation Guide
- Linux Exploit Suggester 2
- Kerberos (I): How does Kerberos work? – Theory
- Fake or Fake: Keeping up with OceanLotus decoys
- RCE on Steam Client via buffer overflow in Server Info
- Analysis for【CVE-2019-5418】File Content Disclosure on Rails
- Digital Forensics Tips&Tricks: How to Detect an Intruder-driven Group Policy Changes
- The pastebin treasure hunter
- Fileless UAC Bypass in Windows Store Binary
- PowerHub: aids a pentester in transferring files bypassing AV

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 over 24 million customers across 100 markets. 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 as an innovation driven company that builds on trust.

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