Security Newsletter

23 December 2019

Subscribe to this newsletter

On the importance of Full Disk Encryption: Payroll Data of 29,000 Facebook Employees Stolen

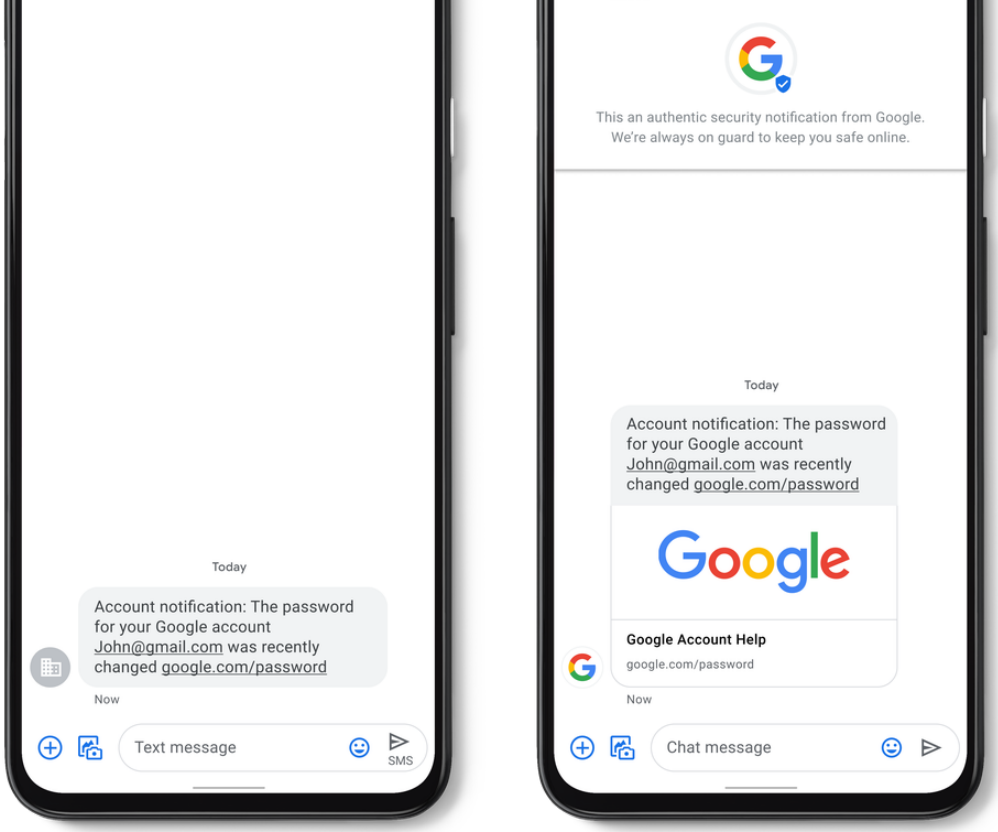
The payroll data of 29,000 current and former Facebook employees was potentially exposed in November when several unencrypted hard disk drives were stolen. The data included U.S. employees' names, bank account numbers and the last four digits of some workers' Social Security numbers, according to an email sent to Facebook employees on Friday, Bloomberg reports. The drives also included some employees' compensation information, including salary and bonus details, according to the news service's report.

In the email to employees, Facebook noted that on Nov.17, someone broke into an employee's car and took the hard disk drives containing the data. It's not clear why the unnamed employee, who works in Facebook's payroll department, had the hard disk drives in their car or why those devices weren't encrypted.

"Out of an abundance of caution, we have notified the current and former employees whose information we believe was stored on the equipment - people who were on our U.S. payroll in 2018 - and are offering them free identity theft and credit monitoring services," the Facebook spokesperson told ISMG. "This theft impacts current and former Facebook employees only, and no Facebook user data was involved."

Read More on BankInfoSecurity

Google adds Verified SMS and anti-spam feature to Messages app



Google announced new security tweaks designed to make old-fashioned SMS communication more appealing to both companies and consumers alike. The first of these is Verified SMS for Messages, which as its name suggests works with the company's Android messaging app. Available in the US, the UK, Canada, Mexico, India, Brazil, France, the Philippines, and Spain, this allows users to verify that text messages sent by companies are genuine and not fakes or scams.

From Google's brief description, every text sent to the Messages app by a participating company embeds a hash-based message authentication code (HMAC) which is compared with an equivalent hash sent to Google. This is unique to each person's device rather than the company itself, which should make it impossible to spoof. As well as being specific to the Messages app, companies must also be part of the Verified SMS system for it to work. So far, that only runs to 1-800-Flowers, Banco Bradesco, Kayak, Payback, and SoFi.

Verified SMS will only authenticate known good senders rather than stopping unknown bad ones. This might explain why Google has added a second feature to Messages, Spam protection for Messages. With this feature in use, any message arriving or leaving from a number not in the user's contacts list is temporarily stored and checked against the numbers of any known spammers If it's suspect, it blocks the message. It's not crystal clear whether this is done automatically or if the user is asked before it is blocked. It's also possible to manually report spam.

Read More on Naked Security

Official Google communication

New Orleans hit by ransomware, city employees told to turn off computers

The City of New Orleans, Louisiana has suffered a ransomware attack that has led to the shut down of the city's servers and computer, but the city states emergency services remain intact. In response to the attack, Nola.com reports that the City told employees to turn off and unplug their computers over the City Hall's public address system. The servers for the city were also shutdown.

According to reports from local media outlets, to make sure employees powered down computers as soon as possible, officials used the city hall's public loudspeakers systems to alert employees of the cyber-attack. Besides city hall, the incident also affected the New Orleans Police Department, which shut down its IT network in entirety as well.

This incident marks the third ransomware incident reported in the state of Louisiana. In August, three school districts were hit by ransomware, prompting the Louisiana governor to declare a state emergency, the first one in the state's history caused by a cyber-attack, rather than a natural disaster. A second incident took place last month when a second ransomware attack encrypted data on the Louisiana state government's IT network. Weeks after the attack, some state agencies are still having difficulties with accessing state data, although these are expected t be resolved by the end of the year.

Read More on ZDNet

Even More on BleepingComputer

This is the last Kindred Security Newsletter for 2019

It's time for the Kindred Group Security team to take some holiday. The newsletter will be off for a few weeks during Christmas and New Year's Eve. But don't worry, we'll be back. See you soon for some awesome infosec news!

More #News

- Apple opens public bug bounty program, publishes official rule
- Ambitious scam wants far more than just PayPal logins
- More than 38,000 people will stand in line this week to get a new password
- Identifying DNS-Over-HTTPS Traffic Without Decryption Possible: Researche
- Google to Force OAuth in G Suite to Increase Securit
- Google Offers Financial Support to Open Source Projects for Cybersecurity
- Over 435K Security Certs Can Be Compromised With Less Than $3,000
- Former Siemens Contractor Sentenced to Prison for Planting Logic Bomb
- Inside 'Evil Corp,' a $100M Cybercrime Menac
- Mozilla: Firefox Add-On Developers Must Use 2F
- Credit Card Data Exposed Online Is Tested Within 2 Hour
- Ring's Hidden Data Let Us Map Amazon's Sprawling Home Surveillance Network
- Droom Fixes Security Flaw That Exposed Private Data, Banking Details of Million
- New Legion Loader Delivers a Variety of Malware
- Who Else Is in That Video Meeting? Maybe a Hacker
- Don't fall for this porn scam – even if your password's in the subject!
- Nuclear Bot Author Arrested in Sextortion Case
- Attackers Steal Credit Cards in Rooster Teeth Data Breach
- 267 Million Facebook Users Exposed in Accessible Database

#Patch Time!

- Drupal Warns Web Admins to Update CMS Sites to Patch a Critical Flaw
- Npm team warns of new 'binary planting' bugs
- TP-Link Router Bug Lets Attackers Login Without Password
- Update Intel's Rapid Storage App to Fix Bug Letting Malware Evade A
- Chrome 79 patched after Android WebView app chaos
- Flaw in Elementor and Beaver Addons Let Anyone Hack WordPress Sites
- Schneider Electric Patches Vulnerabilities in Modicon, EcoStruxure Products

- Cisco Security Appliances Targeted for DoS Attacks via Old Bug

#Tech and #Tools

- Check for Magecart with the Browser
- BeyondProd: A new approach to cloud-native security
- The APIs Malicious Hackers Love to Exploit
- Hacking GitHub with Unicode's dotless 'i'.
- Investigating PrivEsc Methods in AWS
- Out-of-band Attacks
- From dropbox(updater) to NT AUTHORITY\SYSTEM
- Demystifying AWS' AssumeRole and sts:ExternalId
- CanaryTail — a proposed warrant canary standard for automated canary validation
- Persistence – Application Shimming
- 2 New MS security capture any local group/user discovery attempts
- Security Christmas Advent Calendar
- Javascript Anti Debugging — Abusing SourceMappingURL
- SysmonHunter: An easy ATT&CK-based Sysmon hunting tool
- Sysmon Learning Resources
- macOS Native Security Configurations and osquery
- Detecting unsafe path access patterns with PathAuditor

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