Security Newsletter

28 August 2017

"I was hacked": The real (in)security offered by SMS 2-Factors

Let's begin with the assumption that within 24 hours your usual mobile phone number will be hijacked by social engineers. They will use your number to gain access to every account you own that utilizes phone-based authentication and account recovery, like your email. They will then use that access and information to compromise more accounts, and harass, steal, blackmail and extort you and your associates.

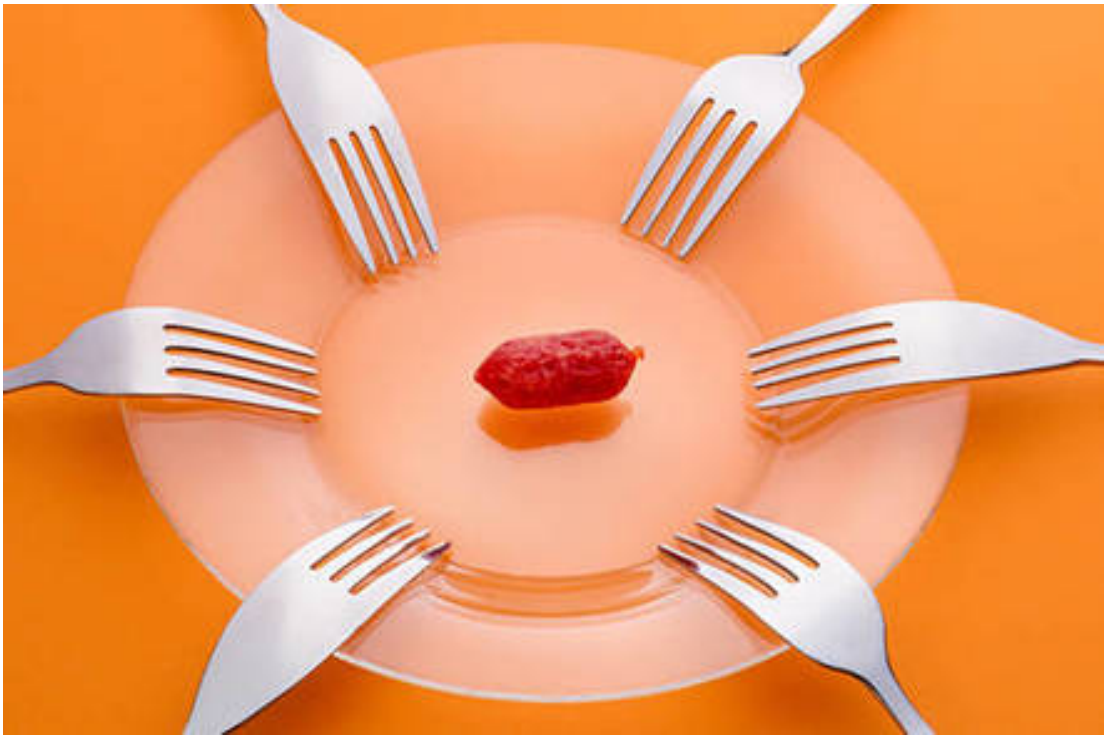
This happen to John Biggs from Tech Crunch: "At about 9pm on Tuesday, August 22 a hacker swapped his or her own SIM card with mine, presumably by calling T-Mobile. This, in turn, shut off network services to my phone and, moments later, allowed the hacker to change most of my Gmail passwords, my Facebook password, and text on my behalf. All of the two-factor notifications went, by default, to my phone number so I received none of them and in about two minutes I was locked out of my digital life."

This trouble is not new, Bitcoin exchange Kraken warns of this and suggests a few tricks to keep yourself safe: Call your telco and set a passcode/PIN on your account, institute a port freeze and a sim lock, add a high-risk flag and close your online web-based management account.

Read More

Kraken Advisory

Cybersecurity world faces 'chronic shortage' of qualified staff



"We are one of the few industries globally experiencing zero-percent unemployment," said Robert Herjavec, CEO of cybersecurity outfit Herjavec Group. "Unfortunately the pipeline of security talent isn't where it needs to be to help curb the cybercrime epidemic. Until we can rectify the quality of education and training that our new cyberexperts receive, we will continue to be outpaced by the Black Hats."

On Sunday, Cybersecurity Ventures predicted that by 2021 there will be 3.5 million vacant cybersecurity jobs due to the lack of a "pipeline of security talent" combined with ever-expanding cybercrime.

Despite record spending on security – and healthy salaries – nearly half of hiring managers say they are struggling to find cybersecurity staff for open positions, and 62 per cent of them have reported a shortage of information security professionals.

Read More

Phish Bait: DMARC Adoption Failures Leave Companies Exposed

More than 90% of Fortune 500 companies have not fully adopted Domain-based Message Authentication, Report & Conformance (DMARC), leaving customers, business partners, and brand names exposed to phishing and other attacks that impersonate corporate email domains.

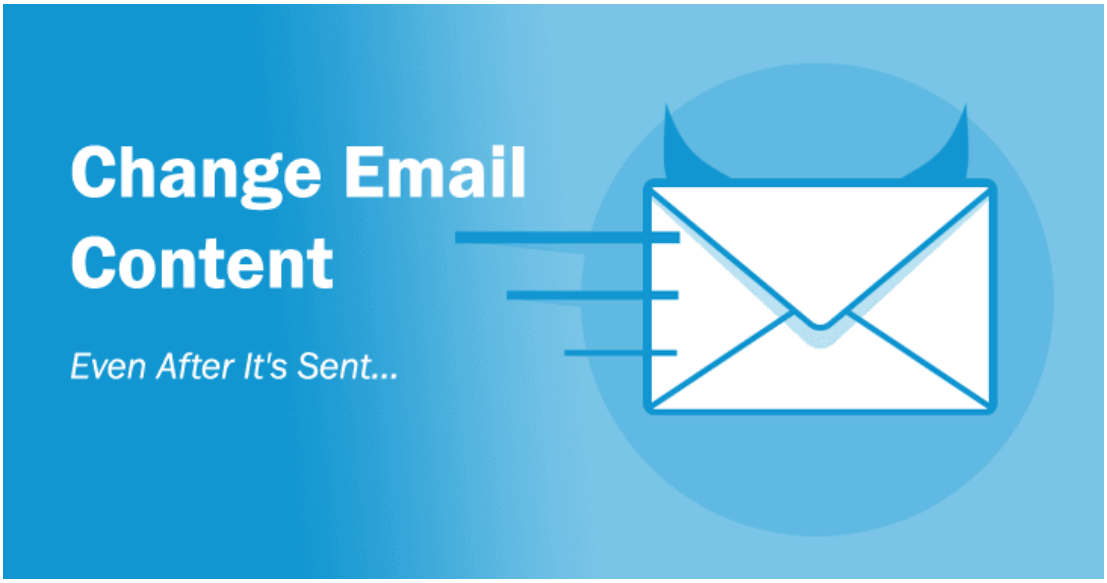
DMARC is a standard technology designed to verify whether an email is from the domain it claims to be from. It creates a whitelist of verified senders, and ensures only authenticated emails are delivered; fake messages are deleted before users see them. It can also be used to see how scammers are misusing corporate information in their attacks.

“Deploying a DMARC policy where p=none is simple, but it is only the first step. Organisations must Quarantine, Reject and maintain strong email governance to reap the benefits of DMARC”, the report concludes.

Read More

DMARC Adoption report

RopeMaker: Debated "vulnerability" allows to modify email content once in your inbox



Dubbed Ropemaker (stands for Remotely Originated Post-delivery Email Manipulation Attacks Keeping Email Risky), the trick was uncovered by Francisco Ribeiro, the researcher at email and cloud security firm Mimecast. A successful exploitation of the Ropemaker attack could allow an attacker to remotely modify the content of an email sent by the attacker itself, for example swapping a URL with the malicious one.

Ropemaker abuses Cascading Style Sheets (CSS) and Hypertext Markup Language (HTML) that are fundamental parts of the way information is presented on the Internet. Since CSS is stored remotely, researchers say an attacker can change the content of an email through remotely initiated changes made to the desired 'style' of the email that is then retrieved remotely and presented to the user, without the recipient, even tech savvy users, knowing about it.

To protect themselves from such attacks, administrators should limit the types of external content that can be loaded automatically via email, in their mail flow policies – this severely limiting the scope of attacks using the methods Mimecast describe.

Read More

Debate over the "vulnerability"

Google bakes in sweeter security for Android Oreo

The Autofill API allows Oreo to better integrate with password managers. While these already work on Android, Autofill allows better support for data such as credit cards and addresses across multiple browsers without the need to enable specific permissions.

Project Treble is a way for smartphones other than Google's own to get software updates (including patches) faster than at present. The gist is that the part of the OS vendors customise is now kept separate from low-level firmware, making it much easier to update.

Finally, Google eschewed the setting for a new 'Install unknown apps' permission that's tied to each app. Android Oreo users will need to grant permission to each app to allow it to download apps from untrusted sources. So, the user could enable Drive and a third-party store app to download apps outside the Play Store, but block Chrome and Gmail from downloading unknown apps.

Read More

Read More

Privacy: Accuweather caught sending user location data without consent

Popular weather app AccuWeather has been caught sending geolocation data to a third-party data monetization firm, even when the user has switched off location sharing. The app would send the Wi-Fi router name and its unique MAC address to the servers of data monetization firm Reveal Mobile every few hours. That data can be correlated with public data to reveal an approximate location of a user's device.

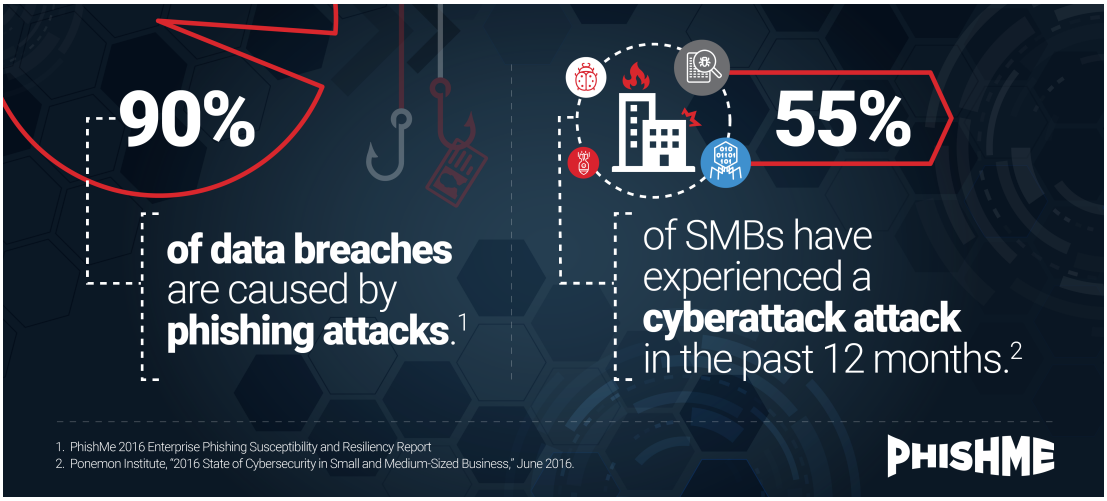
In other words, if you deny AccuWeather permission to use the Location Services APIs on you iPhone, they'll go around your back and send your Wi-Fi router name and the router's MAC address to Reveal Mobile, and they maintain a database that maps Wi-Fi routers to locations.

AccuWeather issued a statement regarding the controversy over their app sending location-identifying information to a monetization firm, which was unconvincing at best. In a further statement, it said it planned to update the app to ensure "zero data" was sent to Reveal Mobile if users opted out of location sharing.

Read More

Even More

PhishMe offers free phishing training tool to SMBs



PhishMe, a 6.5 year old startup that helps companies protect themselves from phishing scams, announced it was releasing a free phishing testing tool for companies with 500 employees or less.

The new tool called PhishMe Free is a cloud service that's a subset of their enterprise product, PhishMe Simulator. The SMB customer simply signs up for the cloud service and PhishMe provides templates that look very similar to recent phishing scams. You can modify it with a company logo to make it look more authentic as you wish, then send it to all your employees, or just a subset.

So what happens when an employee falls for one of the tests? They receive a gentle admonition, explaining that they just fell for a phishing email, and some brief training on how to recognize phishing scams in the future.

This is not the first time Phishme releases awareness content to the community, two years ago, they released free cybersecurity awareness computer based training modules as well.

Phisme Free

Free training modules

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 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and 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