identiverse™

SMS VULNERABILITIES IN IDENTITY MANAGEMENT

BY ROD SOTO

DIR. OF SECURITY RESEARCH

JASK.COM

$Whoami

- Rod Soto
  - Director of Research at JASK.AI, former SPLUNK, AKAMAI, Prolexic PLXSert Principal Researcher. Like to break things, p0wn botnets and play CTFs.

What is SMS?

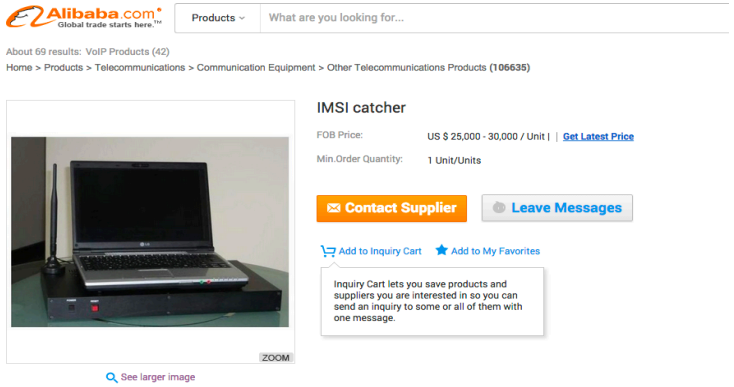
“SMS is a text messaging service component of most telephone, World Wide Web, and mobile device systems. It uses standardized communication protocols to enable mobile devices to exchange short text messages.
“ *Wikipedia

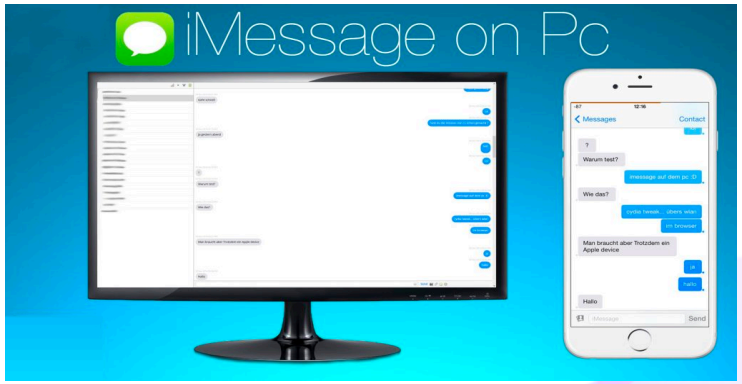
SMS is prevalent in many identity management programs

- Most users have a mobile phone/number. More reliable and economical than tokens.
- SMS widely used as Two Factor Authentication. Simple to use, add on to weak password use.
- SMS has become de facto TFA mechanism. (Microsoft, Google, Twitter, Banks, etc).
- As the phone is always with user, it is assumed that phone proves identity… This is a dangerous assumption.

SMS vulnerabilities in Identity Management

SMS faces a number of attack vectors





identiverse

Main SMS attack vectors

Victim pretexting plays a big part in SMS / ATO attacks

- Malicious actors proceed to call carriers to PORT phone
- Proceed to reset passwords and take over accounts (ATO)
- Go in person to dealers (some might be complicit? Organized Crime?)
- Port when victim is either flying or sleeping or different time zone
- Use google voice numbers to call from foreign countries

** Possession or ability to read SMS is assumed as identity verification*

Main SMS attack vectors

Protection measures are insufficient

- Port Freeze easily bypassed
- Account PIN, secret codes
- Malicious actors call in dozens of times until successful
- Impersonation at dealer *Store clerks not trained or complicit

Main SMS Attack vectors

SMS can be read in devices beyond phone

- Many applications allow reading of SMS text messages in other places .Examples of that functionality can be seen in Google hangouts and Apple iMessage.

- This means, for certain victims, criminals do not need to have access to phone or cellphone signal, they can instead either access online site or compromise computer.

Main SMS attack vectors

TOTP applications can also be bypassed/compromised

Time-based one time passwords algorithms (TOTP), have been suggested as an alternative to SMS two factor authentication. These applications “ compute a one-time password from a shared secret key and the current time”.

identiverse

Main SMS attack tool

Multi Factor Authentication phishing tools

- Phishing is a very powerful attack vector, being currently one of the principal attack vectors against enterprises. The use of misleading messages usually in the form of emails that contain malicious code attached to them, continues to be one of the most used vectors of attacks against enterprises. SMS is primarily used by many enterprises as two factor authentication and to prevent phishing.

- However, as of the writing of this presentation there are already MFA phishing research tools in the infosec community. It is only logical to expect tools like these, applied to crimeware. Further decimating the reliability of SMS as authentication form.

Main SMS attack vectors

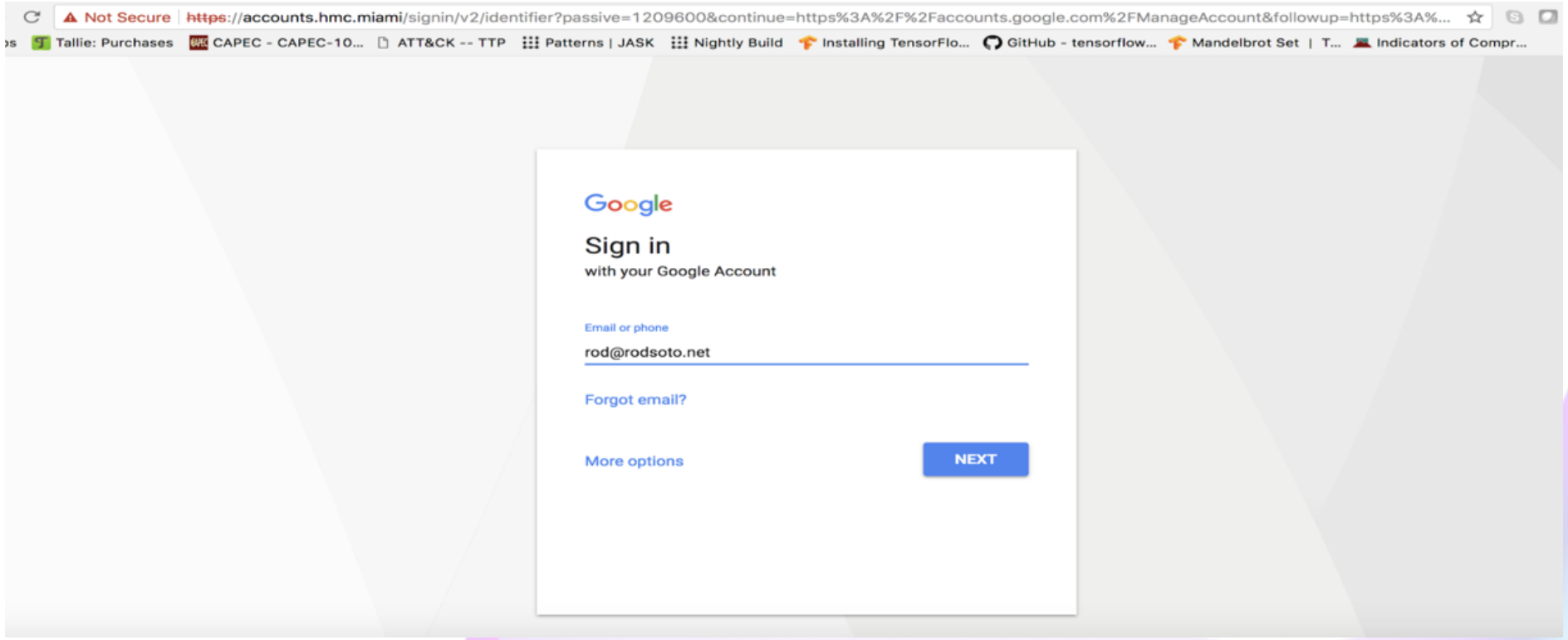
POC Evilginx

```
research@ubuntu:~/evilginx$ sudo python evilginx.py setup -l
                 _ _                  _
                (_) |                (_)
 _____   _____   _| | __ _  _ _ _ _ __ ___  __  __
/ _ \ \ / / | | | |/ _` | | | | | '_ \\ \/ /
|  __/\ V /| | | | (_| | | | | | | |> <
 \___| \_/ |_|_|_|\__, |_|_|_| |_/_/\_\
                   __/ |
 by @mrgretzky    |___/          v.1.1.0

Listing available supported sites:

 - google (/home/research/evilginx/sites/google/config)
   subdomains: accounts, ssl
 - linkedin (/home/research/evilginx/sites/linkedin/config)
   subdomains: www
 - live (/home/research/evilginx/sites/live/config)
   subdomains: login, account
 - facebook (/home/research/evilginx/sites/facebook/config)
   subdomains: www, m
 - icloud (/home/research/evilginx/sites/icloud/config)
   subdomains: www, icloud, edge, setup, idmsa, appleid, id, appcdn
 - dropbox (/home/research/evilginx/sites/dropbox/config)
   subdomains: www

research@ubuntu:~/evilginx$
```

identiverse

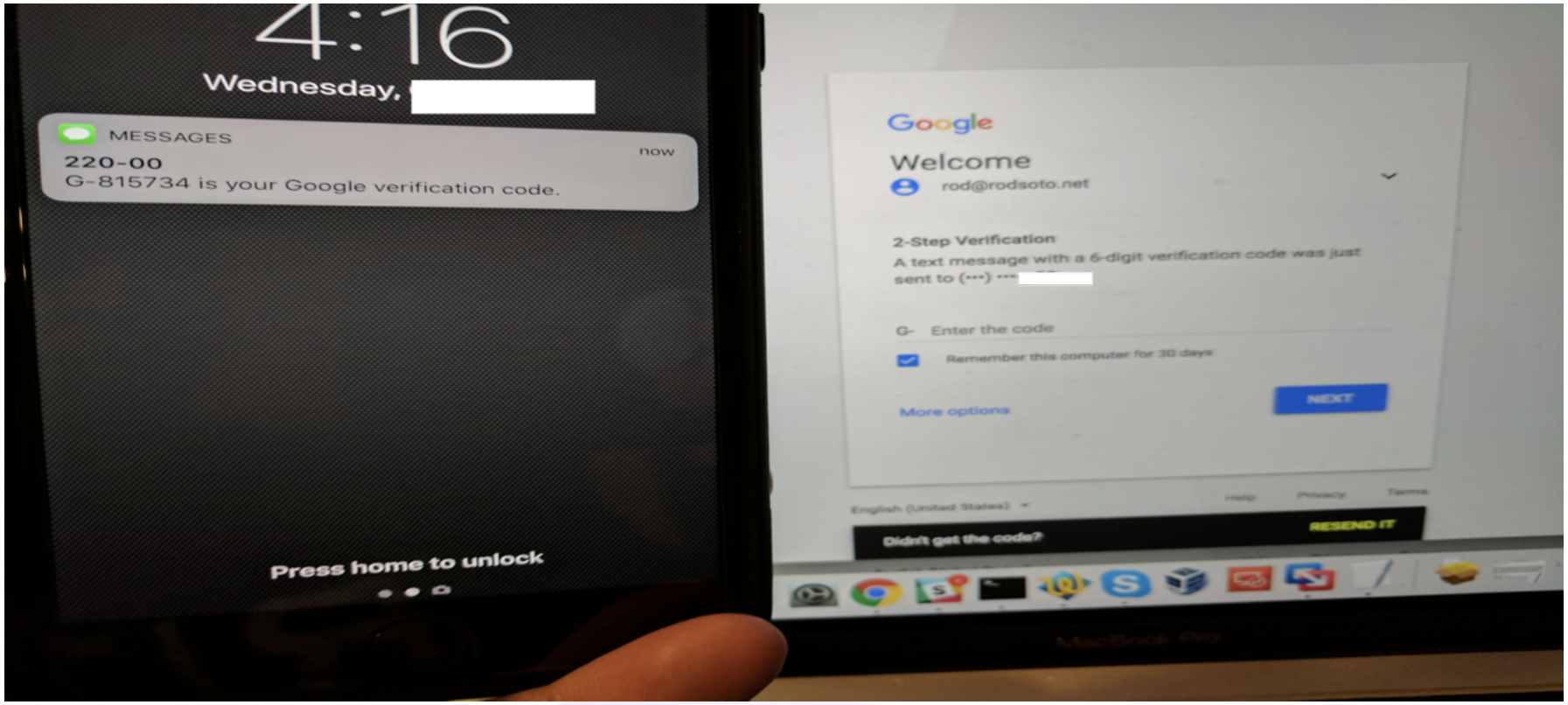
MFA Phishing tool POC

Phishing page/ 2FA prompt and code



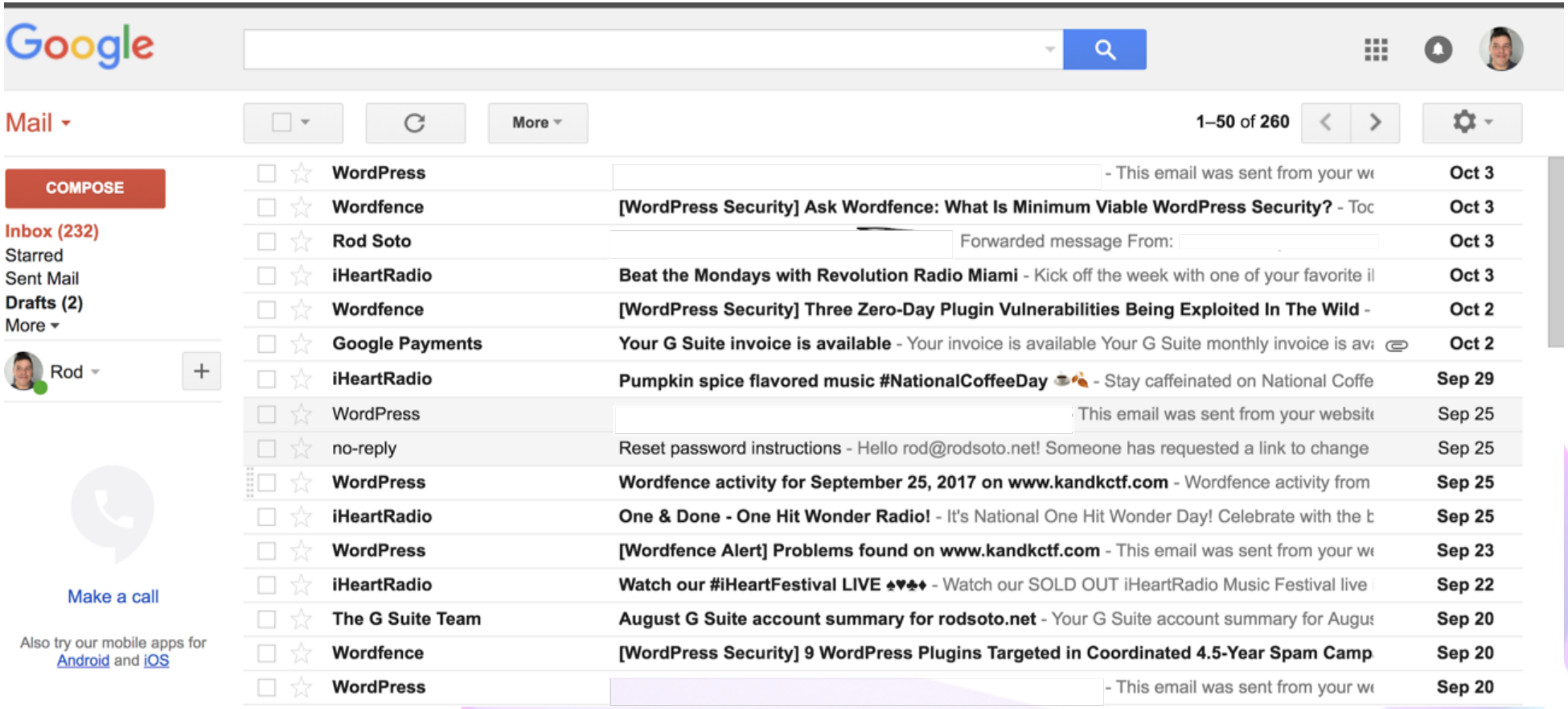
identiverse

MFA Phishing tool POC



identiverse

MFA Phishing tool POC

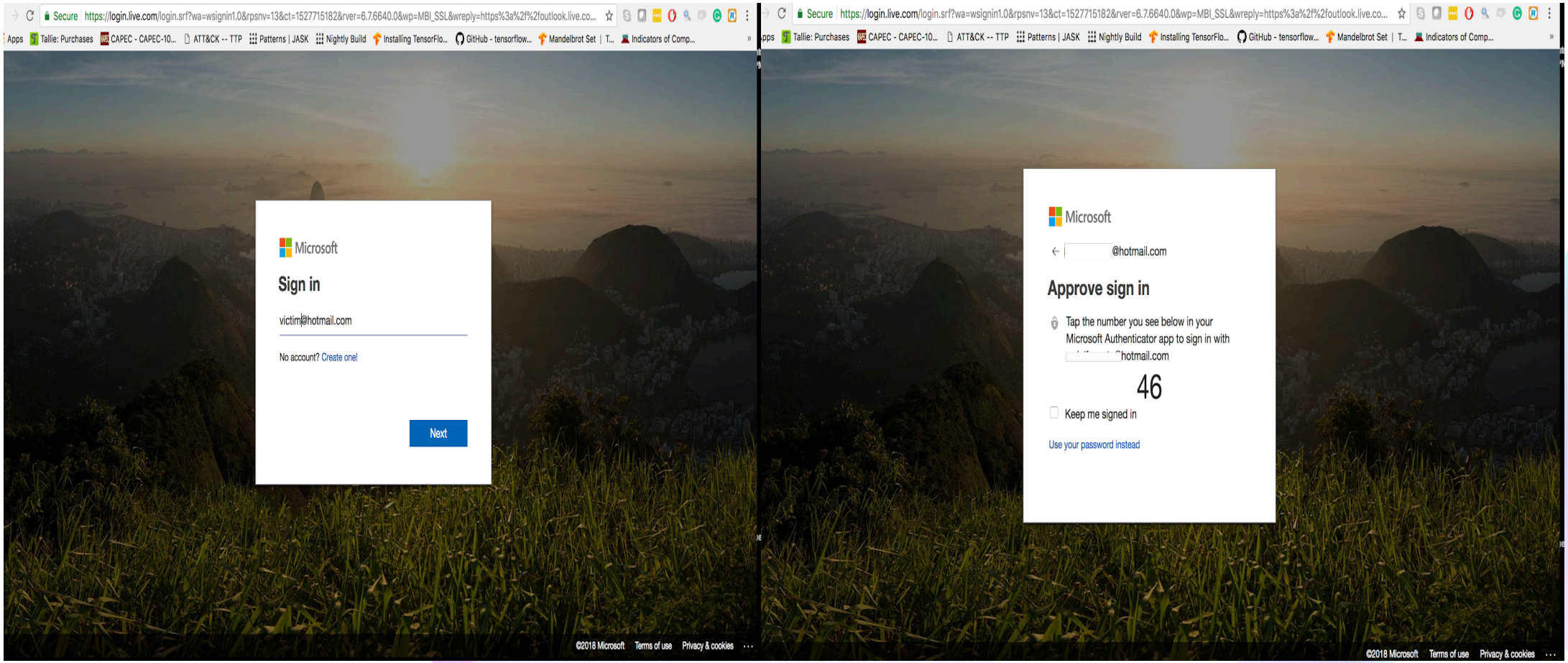


identiverse

Wait there is more..

- TOTP applications can be bypassed too...

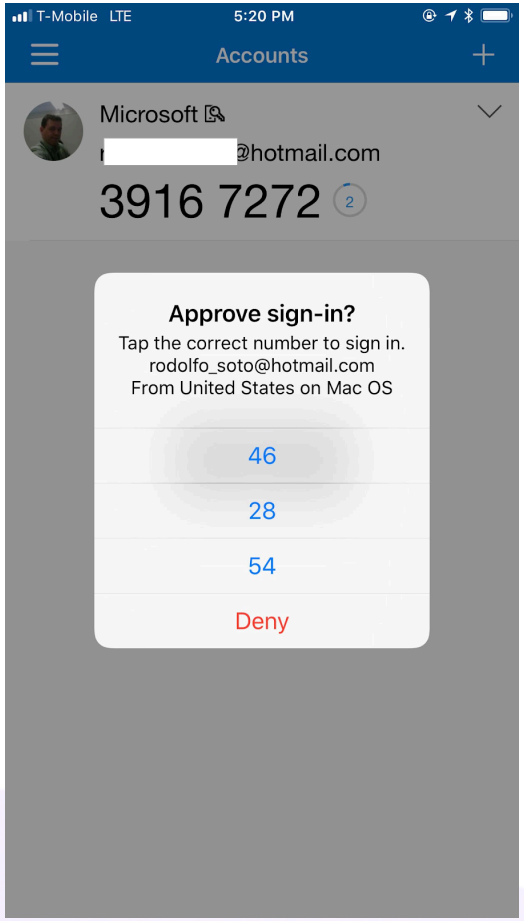
How difficult could it be to hit yes or authorize this?



identiverse

What if you are at lunch, just woke up or at a party?

This scenario just happened at a very large organization.



identiverse

Time to move from SMS

- SMS is not a reliable feature for identity management. SMS vulnerabilities expose not only individuals but organizations.
- The above indicators clearly expose multiple and significant vulnerabilities in the use of SMS as form of authentication.
- Such vulnerabilities establish a scenario where reception of SMS cannot be used to prove identity. The National Institute of Standards and Technologies has advised to deprecate the use of SMS for authentication.
- Cryptocoin community will continue to be targeted. (Meaning EVERYONE that has cryptocoin).

Mitigation

- Current state of this type of authentication method exposes enterprises to a higher risk of compromise due to the possibility of the above mentioned attacks. However, there are certain things that can be done to protect users and enterprises. Some of them include:
- **-- Burner phone for SMS only**
- Some individuals have resorted to purchase phones with numbers to be used exclusively for SMS authentication, keeping their numbers away from public exposure. This may partially protect from pre-texting.
- -- **TOTP -- Time Based One Time Password (google authenticator)**
- Many enterprises are turning into google authenticator as second form of authentication. There are also Microsoft Authenticator and Authy among others.
- -- **Locking features**
- Some enterprises are using “locking”, “freezing”, “delaying” mechanisms in order to give victims enough time to react and claim their accounts, some of these measures include: Coinbase AutoLocking, Apple ID lock, Facebook Extra Security.

Mitigation

- -- **Do not link SMS phone with main email account**
- It creates a single point of failure. Many victims could not communicate with their companies, or services because once attackers obtained SMS they proceeded to change passwords and prevent access from genuine users.
- -- **Tokens**
- If possible use tokens as well as forms of authentication. Username/Password--> TOTP --> Token, like a Yubikey for example.
- -- **Port phone number away from carriers**
- As carriers have shown extremely poor levels of security when it comes to preventing phone porting attacks, many users have discovered that porting phone to things such as Google Voice/Fi makes it extremely difficult to malicious actors to port phone numbers.

Q&A

Rod Soto
rod.soto@jask.com

identiverse