Unspoofable Anti-Phish Codes
Reduce Risk of Data breach & Fraud ~ 0

Girish Chiruvolu, Ph.D., CISSP, CISM, MBA
I changed all my passwords to "incorrect".

So whenever I forget, it will tell me "Your password is incorrect."
Impact Across Every Industry – Phishing, ATO

FACTS & FIGURES

3X
Account takeovers tripled in 2018

$10.6B
Financial fraud loss totaled $10.6 billion in 2018

81%
Credential compromise were at the heart of 81% of the total reported data breaches

$5M
On average, a data-breach cleanup costs at least $5 million

*Javelin, Verizon, Ponemon 2018

THREAT CONTINUES TO GROW
with the increase on sophistication and automation of 2-Factor Phishing

Source: 2018 Identity Fraud Study, Javelin Strategy & Research
Online industries most targeted by phishing attacks as of 2nd quarter 2018*

Why Phishing Works in Practical World?

- It is a numbers game – Probability –0.01% but population set >> millions

- SSL cert padlock – utility severely diminished

https://securelogin.citibank.servicescustomerbanking.dsgdsjgdsjhdshjdsfjhsdjkksdjkjsdfjsdfjkksdkfjsadhgfj.evil.com

Match Top-level-domain. Lock is green, no alert!

Recent real-time proxies (MiM) to impersonate websites
Hey, wait a second...

We have 2-factor authentication!
2-Factor Authentication

My Little Password

We are secure!
Welcome Advanced 2FA Phishing Automation

Phishing with 2FA enabled (Evilginx 2)
DemmSec • 8.9K views • 5 months ago
Learn how to set up Evilginx2 which can be used to phish a target even if they have 2FA enabled. The contents of this video are ...

1/17/19 Modlishka Tool Automates Phishing Attacks, Bypasses 2FA | AT&T ThreatTraq
AT&T Tech Channel • 1.7K views • 2 months ago
http://go.att.com/d45310ab Originally recorded January 17, 2019 AT&T ThreatTraq welcomes your e-mail questions and feedback ...

Organizations are implementing two-factor on more and more web services. The traditional methods for phishing credentials is no ...

New Exploit Hacks LinkedIn 2-factor Authentication
KnowBe4 • 51K views • 10 months ago
Kevin Mitnick shows how the exploit is based on a credentials phishing attack that uses a typo-squatting domain. Once the user ...
Welcome Advanced 2FA Phishing Automation!

Tokens
(One-time Codes)

SMS Approval
(Out-of-Band)
Current 2nd Factor Authentication Space
All are vulnerable to Credential Harvesting and Account Compromise

MAN-IN-MIDDLE
PHISHING
OVER-THE-SHOULDER
KEYLOGGER MALWARE
How it Works: Account Takeover
Account takeover after victim follows phishing link with current 2-factor authentication

Regular Token Scenario

Victim
- Requests Login Page
- Login Page Served
- Submits Credentials (including 2FA)

Man-in-Middle Proxy Server

Authentication Server
- Proxies Login Request
- Login Page Served
- Proxy Submits Credentials

ACCOUNT TAKEOVER

Verifies & Accepts Credentials (sets Authenticated state cookies)
Equivalent in Credential Stealing

**SCENARIO A**
- **Victim**
- **Man-in-Middle Proxy Server**
- **Authentication Server**

**SCENARIO B**
- **Simulate This**

**Steps**
- **Step 1**: Snoop on Victim Passcodes
- **Step 2**: Uses the Snooped Passcodes to Login
Time for a Hack!
Let's Play ...
Account takeover through stolen credentials with anti-phishing codes

First logs-in with the codes displayed

Steals the displayed codes and logs-in

First, we use regularotp - Google Auth

Next, we use secureotp – Bearer-aware OTP
Logged-in with Spoofed Credentials?

Password and Regular OTP were perfectly Interceptable and Spoofable for Account Take-Overs

Bearer-Agnostic

One who holds the bill can spend it!
Bearer-Sensitive OTPs

End-Devices are not lost or stolen

End-Devices are not compromised – NOT Rooted, Jail-broken with Malware
How it Works: No Account Takeover
BOTP Anti-Phish Codes Prevent Account Takeover

Victim

Requests Login Page
Login Page Served
Submits Bearer-Sensitive OTP

Man-in-Middle Proxy Server

Proxy Submits Credentials
Verifies who is the Bearer in addition to proof-of-shared secret
Rejects credentials
NO authenticated state cookies

UberPasscodes® Authentication Server

Proxies Login Request
Login Page Served

NO ACCOUNT TAKEOVER

Victim

Victim Man-in-Middle Proxy Server

Victim

Victim
Equivalent in Credential Stealing

**SCENARIO A**
- Victim
- Man-in-Middle Proxy Server
- Authentication Server

**SCENARIO B**
- Snoop on Victim Passcodes (Step 1)
- Uses the Snooped Passcodes to Login (Step 2)
- Authentication Server

Simulate This
How it Works: No Account Takeover

Anti-Phish Codes Prevent Account Takeover

Victim

Requests Login Page

Login Page Served

Submits Bearer-Sensitive OTP

Man-in-Middle Proxy Server

Proxies Login Request

Login Page Served

Proxy Submits Credentials

Verifies who is the Bearer in addition to proof-of-shared secret

Rejects credentials

NO authenticated state cookies

NO ACCOUNT TAKEOVER
Logged-in with APC Spoofed Credentials?

Anti-Phish BOTP, When intercepted and spoofed, the system detects and stops the session transition into authenticated state.

Thus no account-take-overs.
<table>
<thead>
<tr>
<th>UberPasscodes® vs. FIDO2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No Capex</strong></td>
</tr>
<tr>
<td>UberPasscodes®</td>
</tr>
<tr>
<td>Fido U2F/A</td>
</tr>
</tbody>
</table>
Summary Anti-Phish Codes

**BY DESIGN**

User cannot go to a phishy website and lose credentials

Credential Phishing attacks made ineffective

Eliminate Data breaches and Fraud due to Credential Compromise

81% of data breaches and online fraud start with credential compromise

Bearer-sensitive one time passcode (BOTP) address them!

Cheaper and s/w (app) based - No hardware dongles needed
Thank you!

For White Paper & Exploring more

info@uberpasscodes.com

1400 Preston Rd, Suite 400
Plano, TX 75093

T: 1-(888)-240-8461
info@uberpasscodes.com
https://uberpasscodes.com/