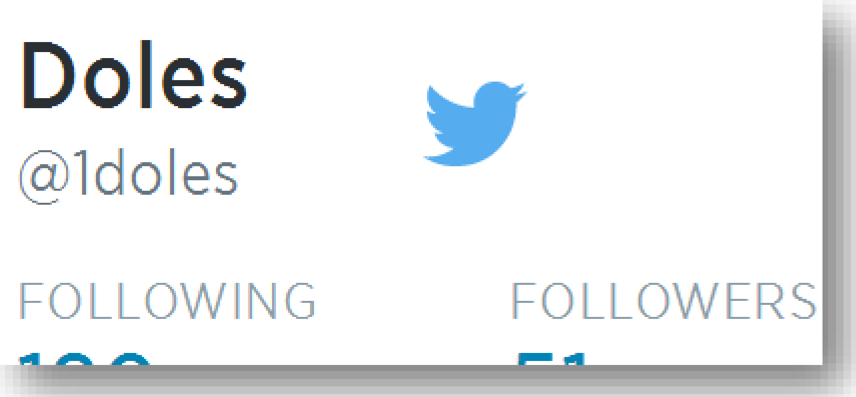
Get out the way, 2FA

About Me

Alex Dolan

a@adolan.info



Doles

@1doles

FOLLOWING

FOLLOWERS

- Is new
- Is from South West
- Works @CNComputers by day
- Drops hard infosec truths on businesses by night

Using the side door

2FA

- Two Factor Authentication is not a blanket solution
- It needs to be tested thoroughly

Mobile Sites

- Consider more testing
- Does it share authentication with the main web app?

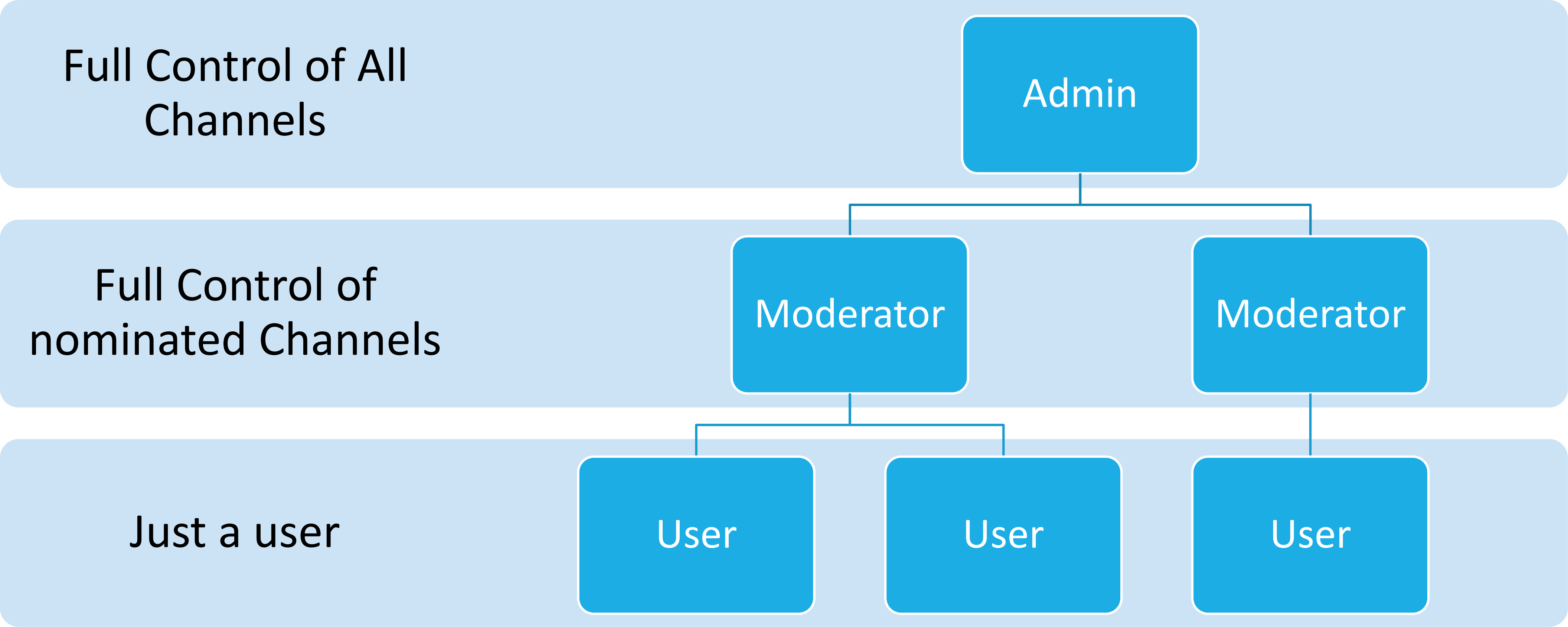
Meet MMGN

- Australian
- Online gaming and media community website
- Est 2005 as “PSPgo”
- Over 50,000 members
- Forums and news stuff
- Completely custom built.

Meet MMGN’s sites (Channels)

- mmgn.com
- wii.mmgn.com
- answers.mmgn.com
- gallery.mmgn.com
- pc.mmgn.com
- tv.mmgn.com
- movies.mmgn.com
- 360.mmgn.com
- ds.mmgn.com
- market.mmgn.com
- anime.mmgn.com
- bidforkids.mmgn.com
- retro.mmgn.com
- vita.mmgn.com
- music.mmgn.com
- ps3.mmgn.com
- apple.mmgn.com
- apb.mmgn.com
- psp.mmgn.com
- yougettheidea.mmgn.com
- Therearealotofsubdomains.mmgn.com

Meet MMGN’s Privilege Structure

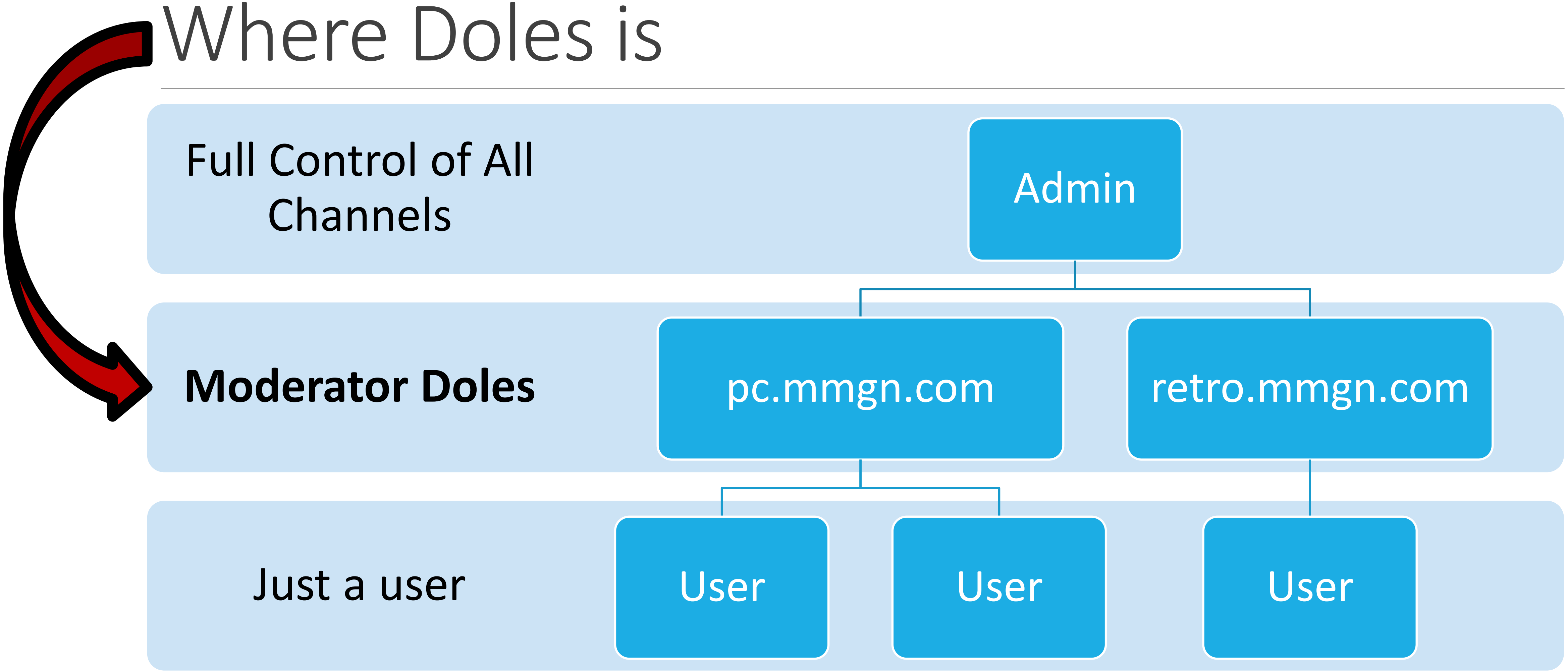


Full Control of All Channels

Full Control of nominated Channels

Just a user

Where Doles is

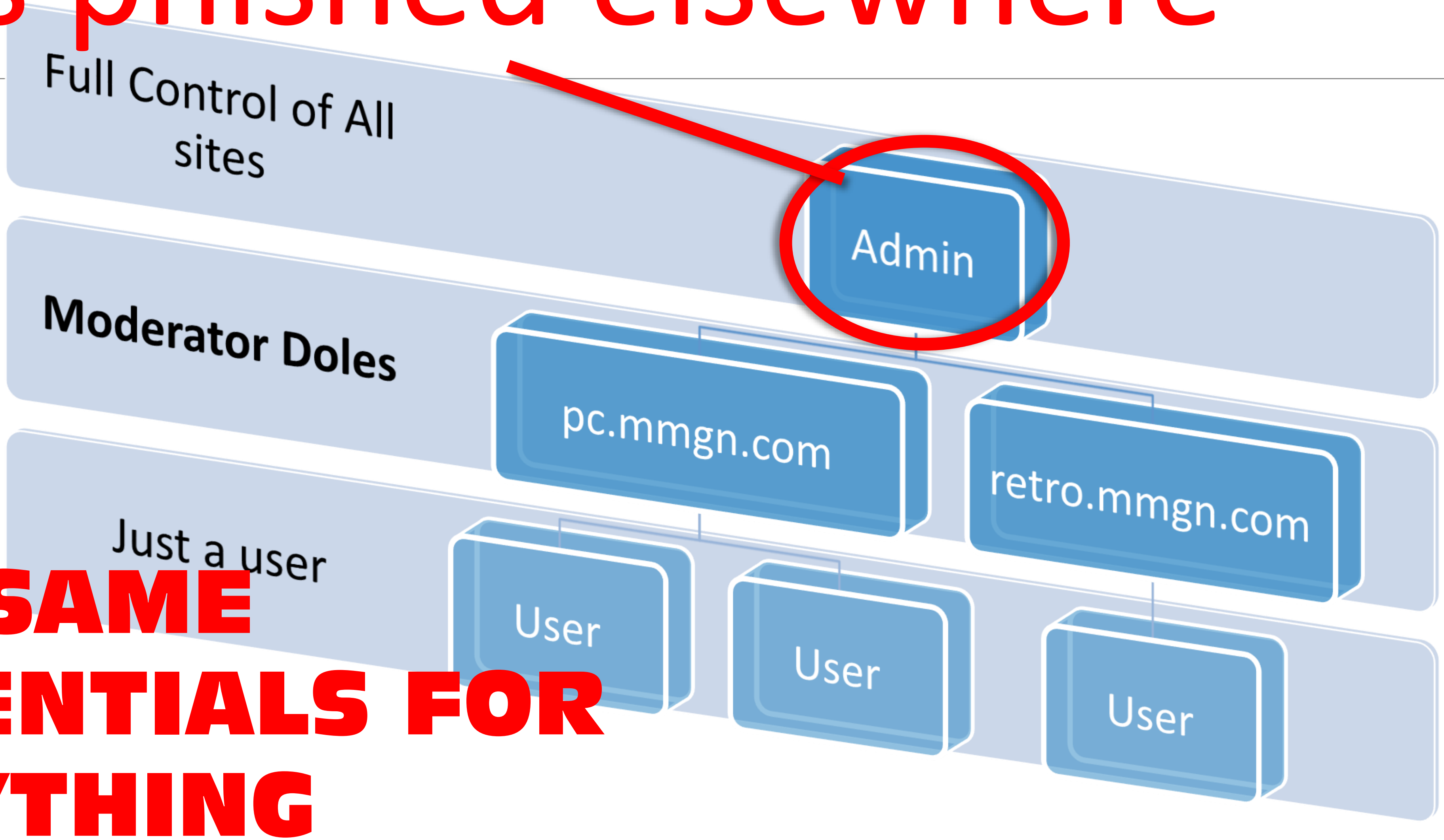


Full Control of All Channels

Moderator Doles

Just a user

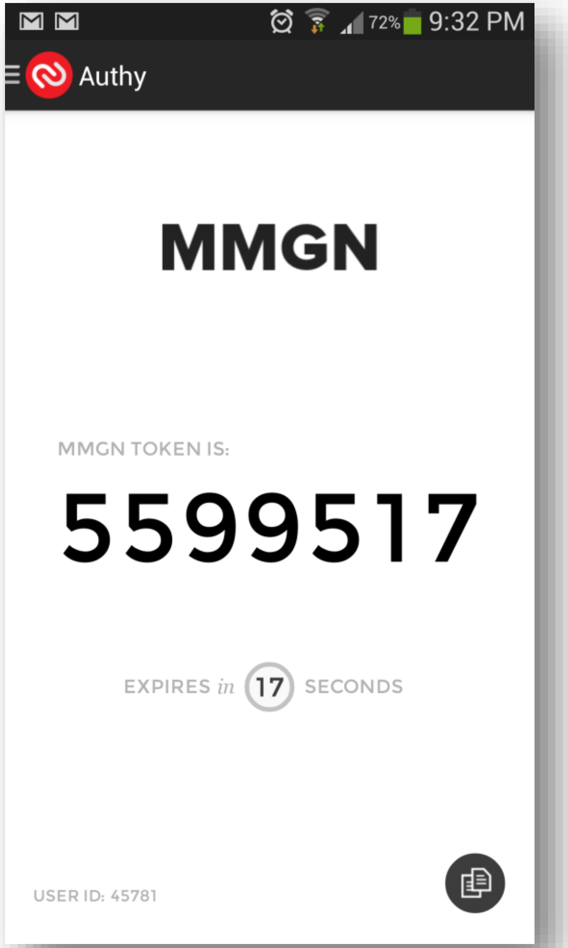
Gets phished elsewhere



USES SAME CREDENTIALS FOR EVERYTHING

Introduce 2FA to mitigate compromise

AUTHY



72% 9:32 PM

Authy

MMGN

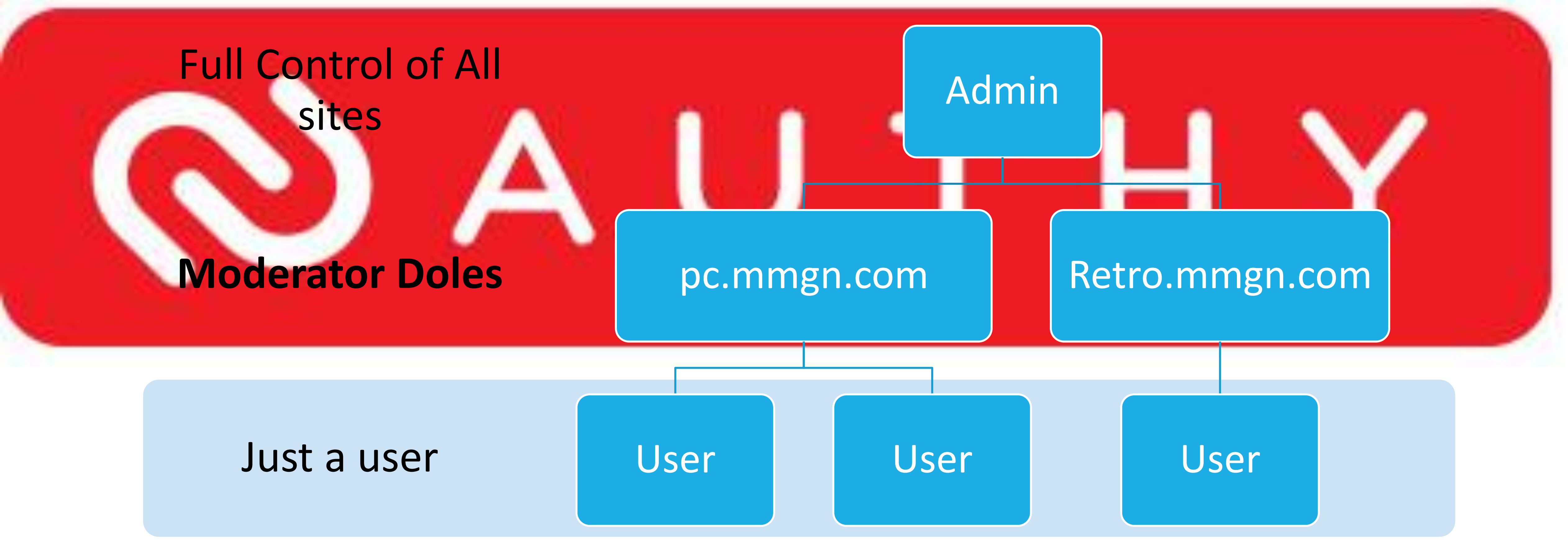
MMGN TOKEN IS:

5599517

EXPIRES *in* 17 SECONDS

USER ID: 45781

Where I am



Full Control of All sites

Moderator Doles

Just a user

Admin

pc.mmgn.com

Retro.mmgn.com

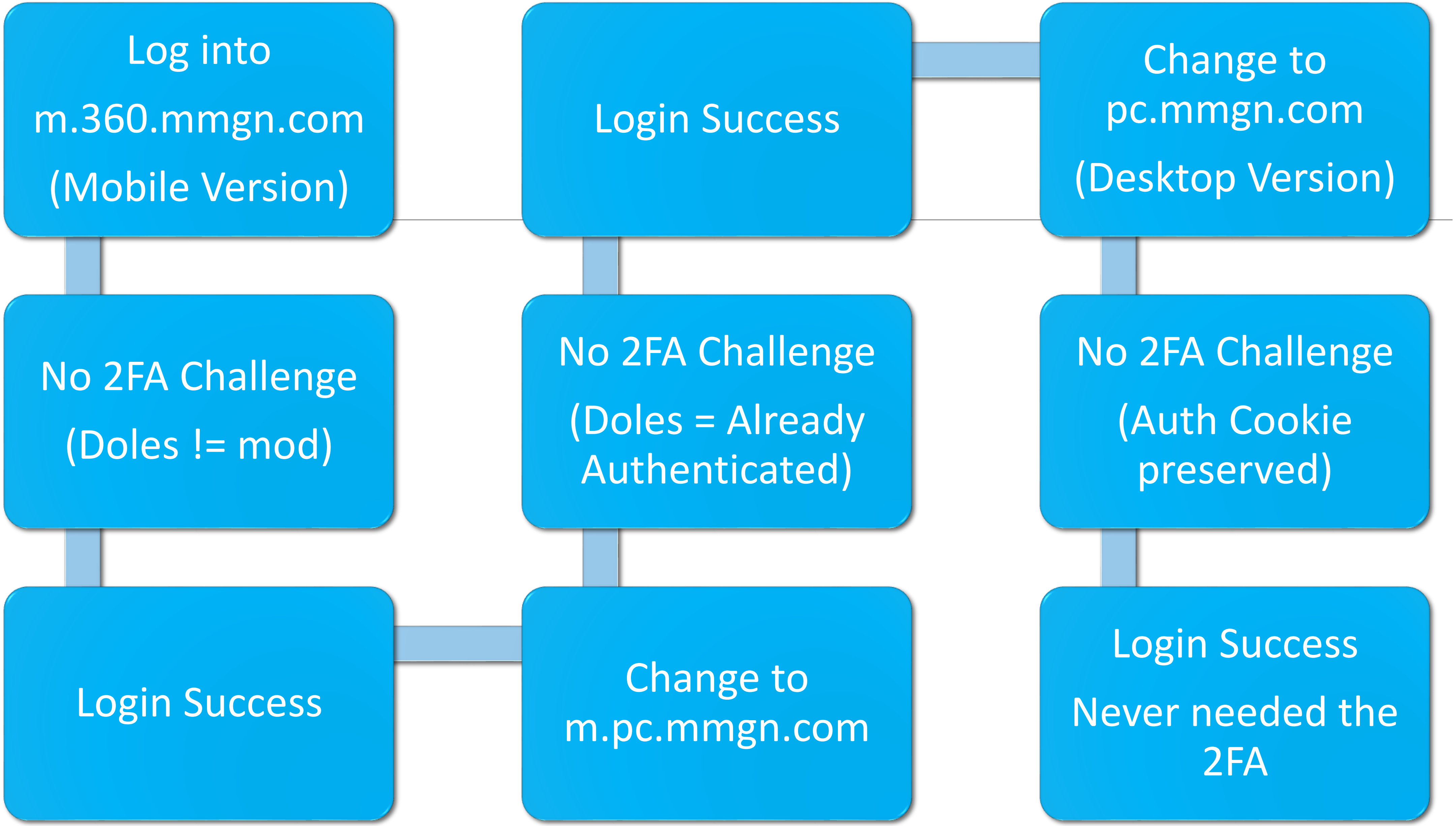
User

User

User

Bypassing 2FA

- Extremely Simple
- Issue fixed within a week of reporting (Oct 2013)
- Not enough documentation taken at the time ☹



Log into m.360.mmgn.com (Mobile Version)

No 2FA Challenge (Doles != mod)

Login Success

Change to m.pc.mmgn.com

No 2FA Challenge (Doles = Already Authenticated)

Login Success

Change to pc.mmgn.com (Desktop Version)

No 2FA Challenge (Auth Cookie preserved)

Login Success Never needed the 2FA

Why did that work?

- Again, not enough documentation taken
- Mobile site shares Post-Authenticated session with desktop site
- Not asked to re-auth when changing to a mod-enabled site
- Different Channels don’t require 2FA – depending on Moderator

What would have fixed it

- 2FA required for any user who is a moderator on any site.
- Global Authentication across mobile/desktop – either share the

auth system or don’t share the cookies

Thoughts for Attackers

- More consideration of the mobile version
- Is there a way around the 2FA?
- When are you NOT asked for the token?

Thoughts for Defenders

- 2FA not a blanket solution
- 2FA poorly implemented = no 2FA at all
- Needs to be tested properly

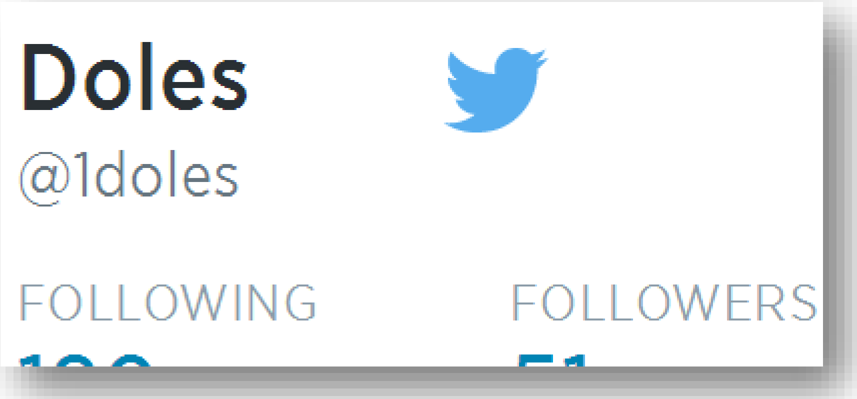
Thanks!

Alex Dolan

Information Security Solutions

Training | Testing | Consulting

a@adolan.info



Doles

@1doles

FOLLOWING

FOLLOWERS