
SecTheory
Internet Security

33 Minutes On the Clock Please…

- We all hear about anti-phishing gadgets that cost an arm and a leg.
- I'm here to tell you why you'll pay for it, even though it doesn't work.
  - Because you're going to fall into the trap, just like everyone else. Plan to fail now.
- Let's get on with it.





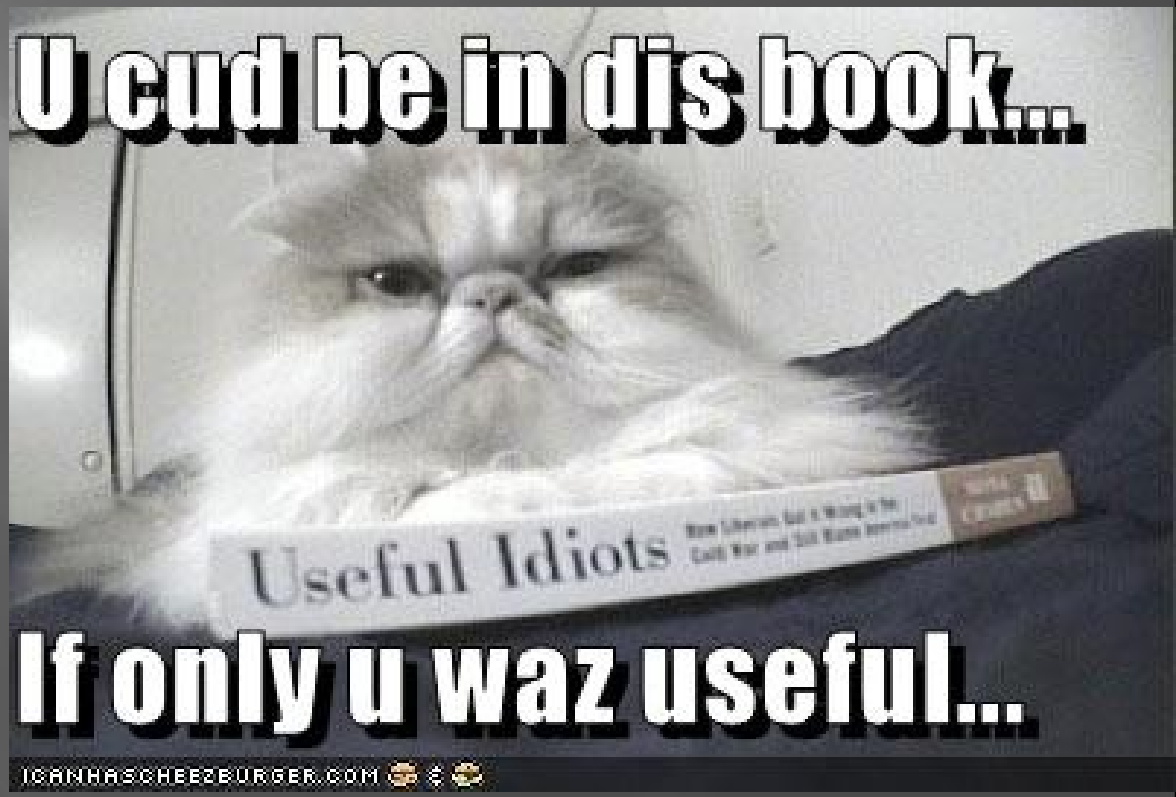
2nd Factor Auth

- "Please mail us your username, password and token."
- People won't federate
- People lose them, type them in backwards, etc... etc...
- Can anyone beat the record of 13 keyfobs?!



.bank TLD

- Hackers don't use .bank and no one notices anyway.
- Only banks can use it? Can I have .momandpa pls?
- Wait, why again are we building another EV Cert?



SSL EV Certs



- Phishers don't use SSL
- Prohibitively expensive for ma and pa retailers
- Users don't get it anyway
- Look for the lock messaging is lost

GridMark

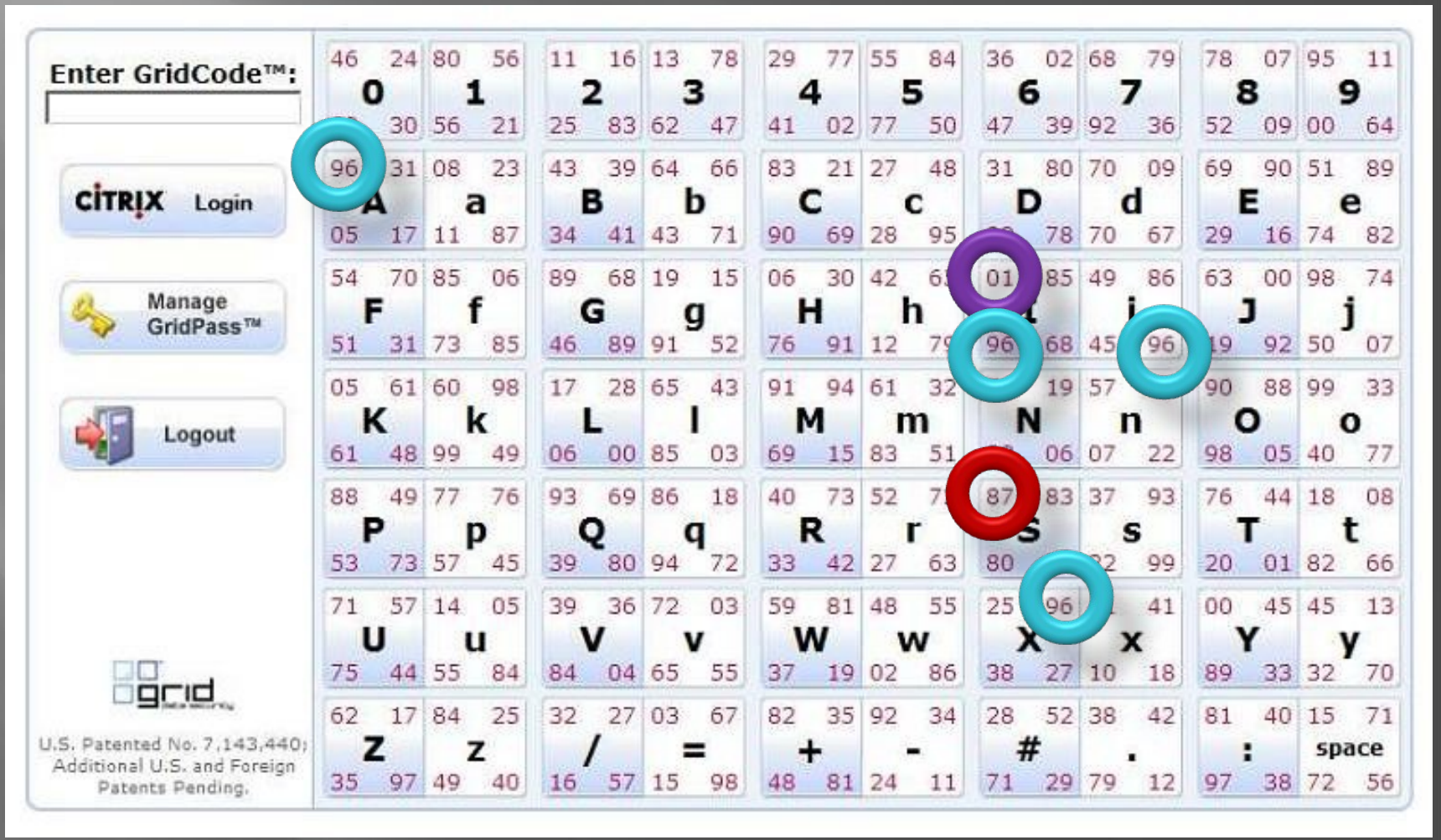
GridOne

01878796

01 87 87 96

ISSA

Snake oil



SiteKey

- MIT study – People don't notice if it's changed or even not there at all!
- Man in the middle attacks
- Phishers can simply say, "We lost your sitekey image, could you pick a new one, kthksbye"



And Anyway…

- The vast majority of trusted sites still have:
  - XSS
  - CSRF
  - SQLInjection
  - Command injection



Most Enterprises…

- Don't use any sort of email, phone or FAX encryption with their customers/clients
- Don't have any brute force detection (or if they do, only vertical)
- Don't force strong passwords, auto log out, automatic password change, etc...
- Do have downloads over HTTP! Weee!



Yup, that's right, you heard me.



- Yup, you're going to pay for all those same nearly pointless security doo-dads even though you haven't fixed any of your other issues!

Wait, why will I pay for this crap?

- Bear analogy. (I hate that analogy, btw). We are bidding up our security.
- Yes, you will probably buy snake oil, just like everyone else.
- Can you blame the vendors for monetizing our problems with the latest security widget?
- Plan to fail - you're probably already doing it!

