Cyber Security

How can we keep our data secure?

Put your white hat on

Authentication

- **Ownership** Factors - something the user *has*
- **Knowledge** Factors - something the user *knows*
- **Inherence** Factors - something the user *is*

Passwords

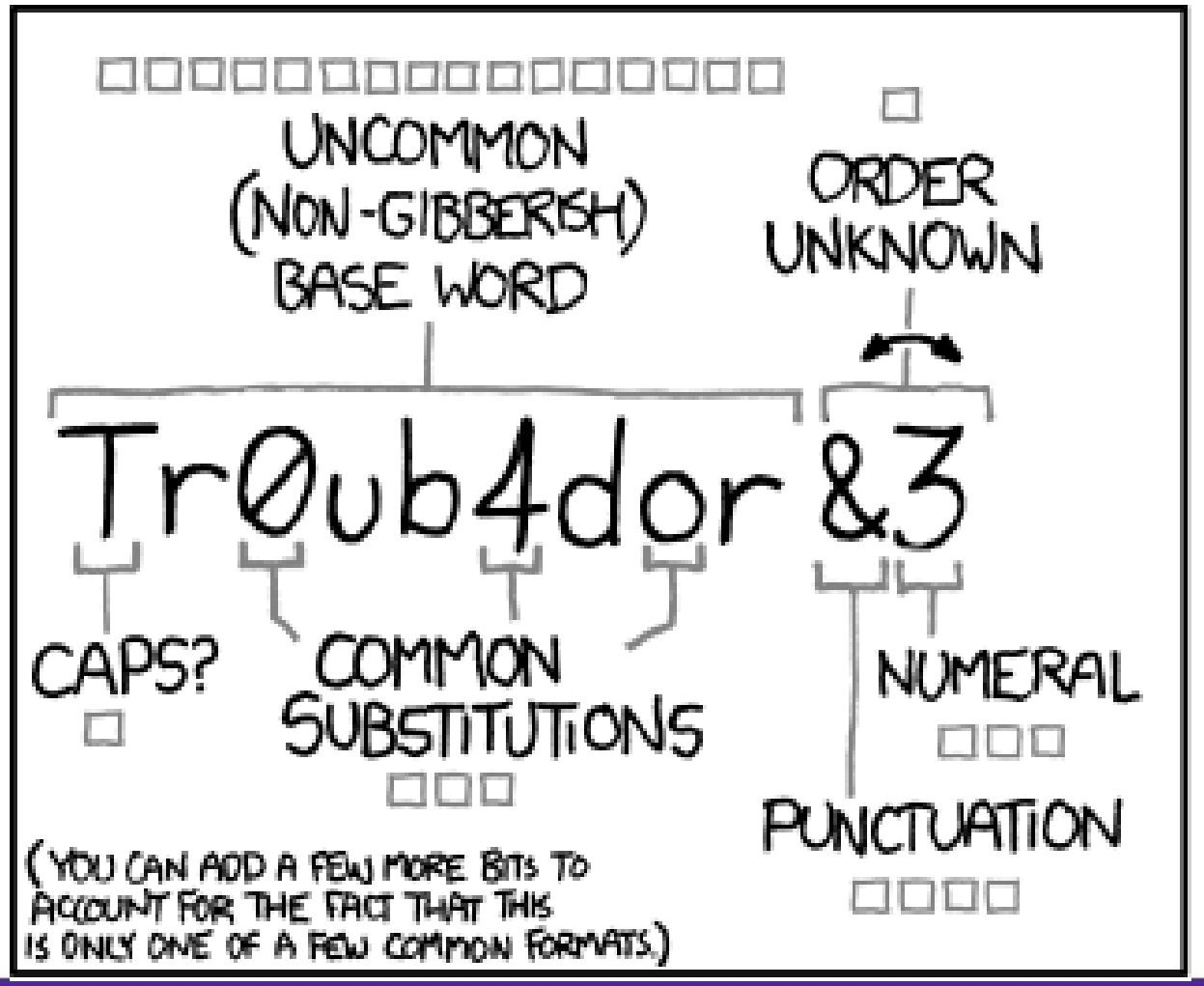


Image Source: XKCD

Cracking Passwords – Brute Force

- aaaaaa
- aaaaab
- aaaaac
- aaaaad
- aaaaae
- aaaaaf
- aaaaag
- aaaaah
- aaaaai
- aaaaaj
- aaaaak
- aaaaal
- aaaaam
- aaaaan
- aaaaao
- aaaaap
- aaaaaq
- aaaaar
- aaaaas
- aaaaat
- aaaaau

Rainbow Tables

1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. sunshine
9. qwerty
10. iloveyou
11. princess
12. admin
13. welcome
14. 666666
15. abc123
16. football
17. 123123
18. monkey
19. 654321
20. !@#$%^&*
21. charlie
22. aa123456
23. donald
24. password1
25. qwerty123

Source: Gizmodo

Password Entropy

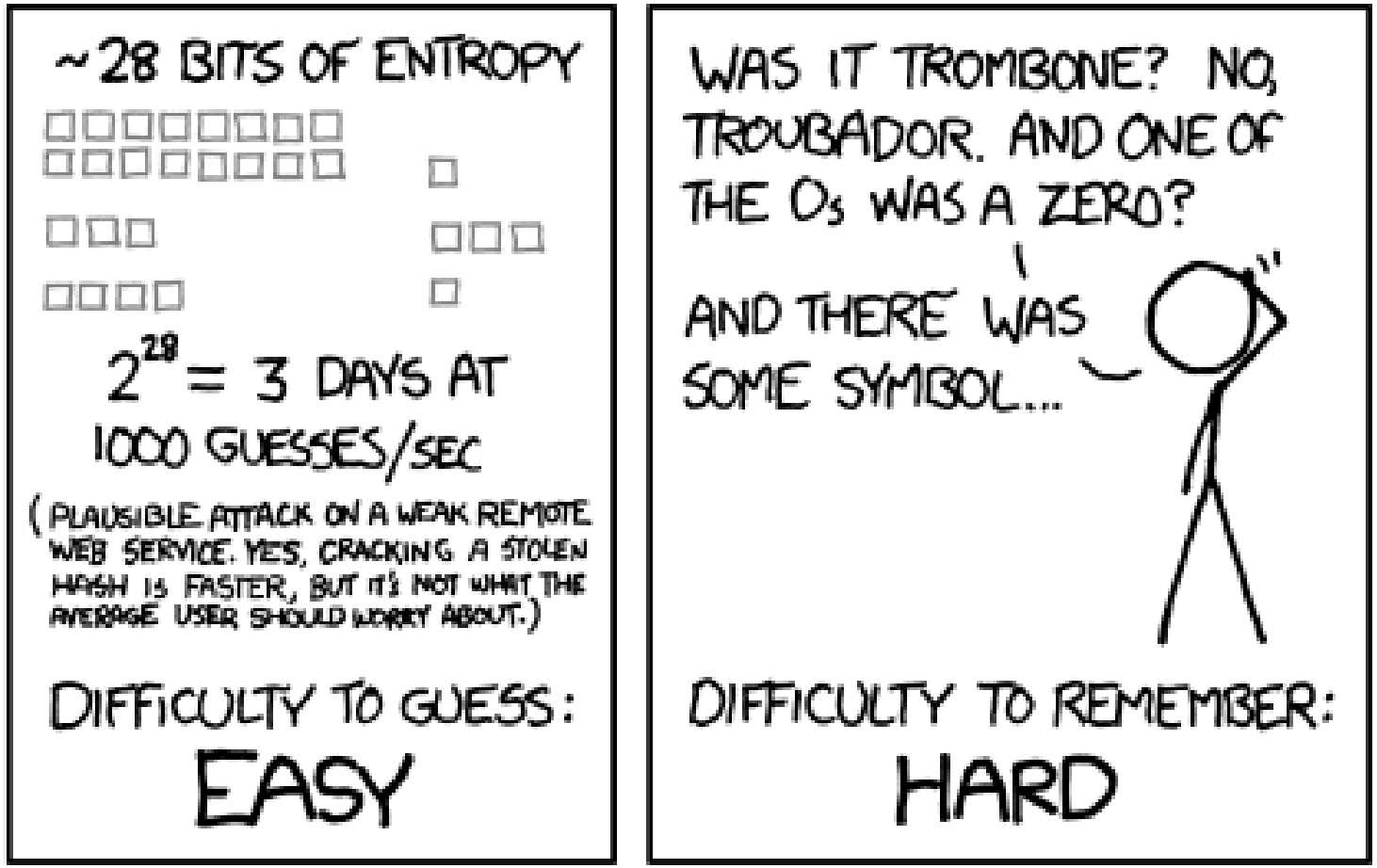


Image Source: XKCD

Password Entropy

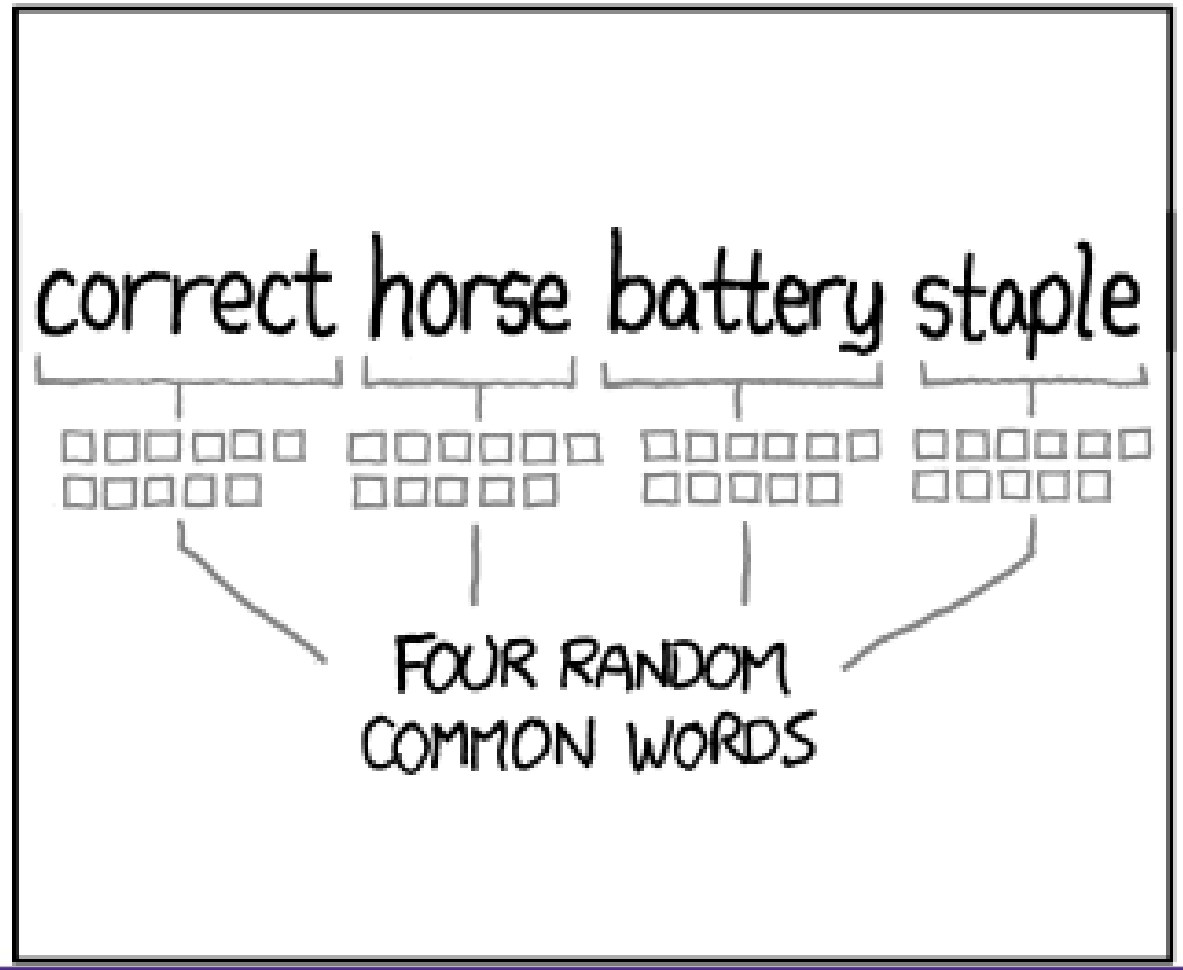


Image Source: XKCD

Password Entropy

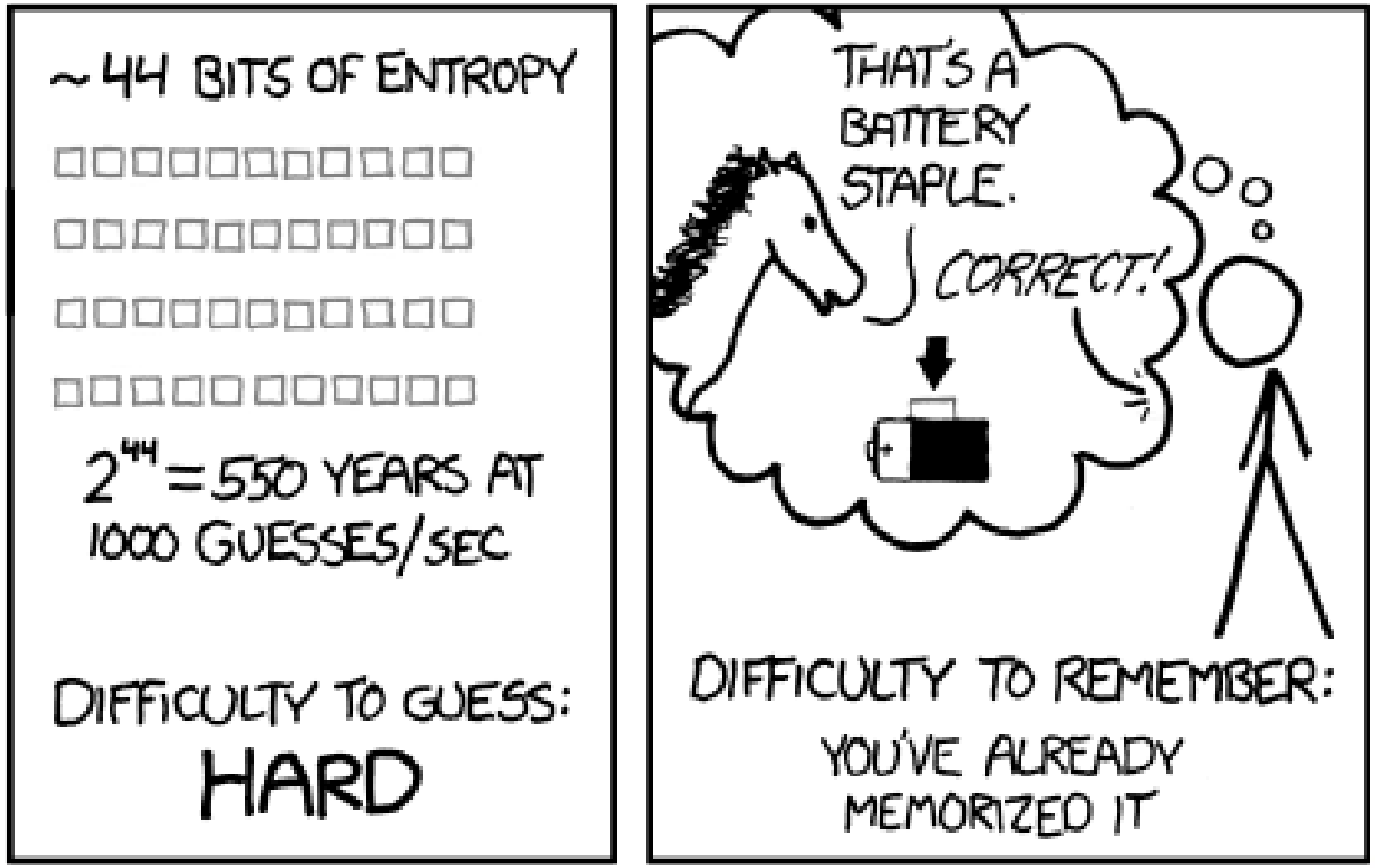


Image Source: XKCD

Storing Passwords Securely

Store the password itself

- Needed to compromise: database access
- Accounts compromised: all
- Relative ease: simple

Storing Passwords Securely

Encrypt all passwords with a key

- Needed to compromise: database & key (or lookup table)
- Accounts compromised: all
- Relative ease: medium

Password Salt

- Random data added to a password before hashing
- Protects against dictionary and rainbow table attacks
- Ensures the password is long enough to be hard to crack

Storing Passwords Securely

Encrypt all passwords with a global salt value

- Needed to compromise: database, encryption key & salt value
- Accounts compromised: all
- Relative ease: harder

Storing Passwords Securely

Encrypt all passwords with a unique salt value

- Needed to compromise: database, encryption key & salt value
- Accounts compromised: one at a time
- Relative ease: really hard

MD5 Hash

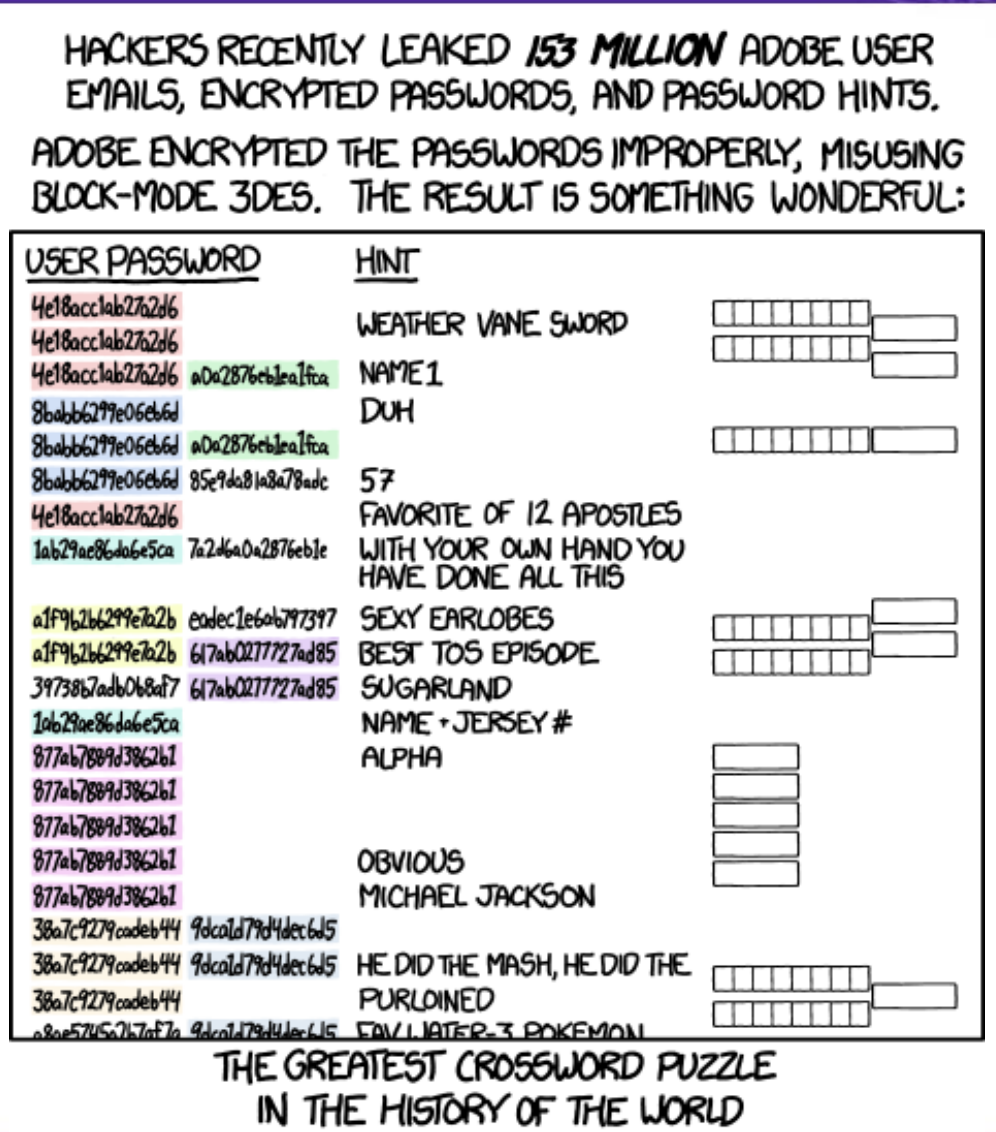


Image Source: XKCD

How Secure is your Password?

https://howsecureismypassword.net/

Social Engineering

Using techniques to compromise a system by exploiting the users directly instead of the system's security

Image Source

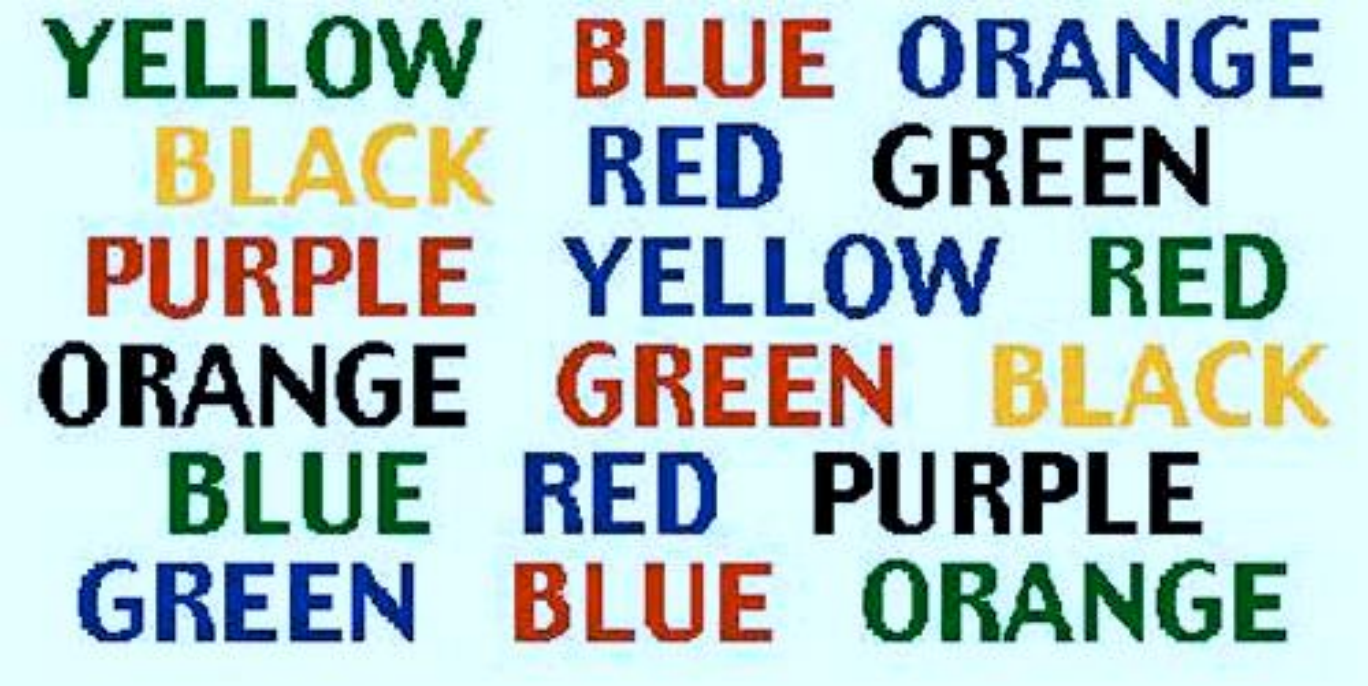
Pretexting

Image Source: Penetration Test Lab

Impersonation

Image Source: 1worder

Human Buffer Overflow



Psychological Principals: The Human Buffer Overflow. Social-Engineer, 22 Dec. 2009. Web. 27 Nov. 2011.

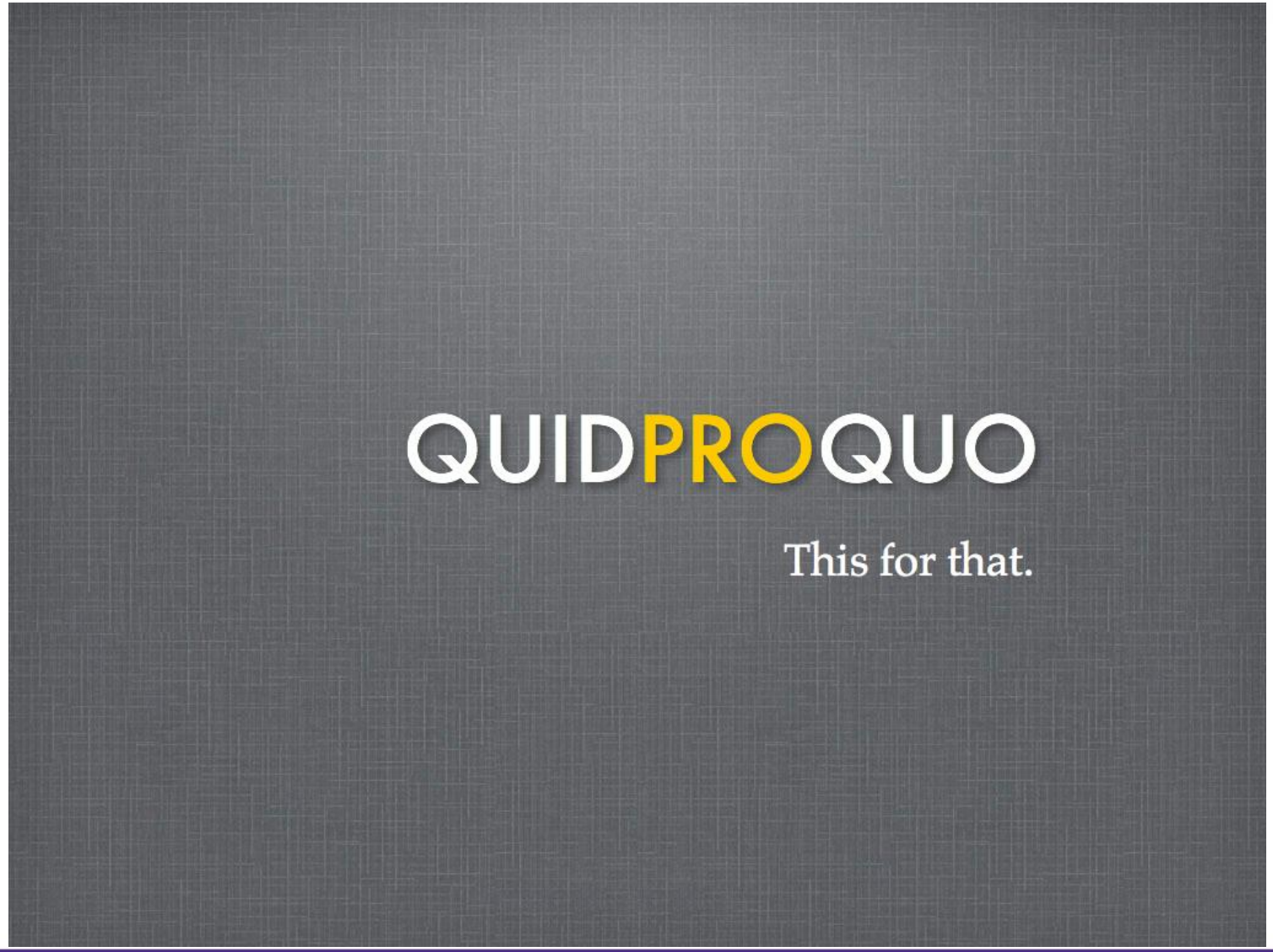


Image Source: John Gosier on Flickr

Phishing

KSU.EDU WEBMAIL TEAM SUPPORT UPDATE/MAINTENANCE OF USER ACCOUNT

© Kansas State University WEBMAIL TEAM <accountupgrade@ksu.edu>

Extra line breaks in this message were removed.

Sent: Thu 4/4/2013 12:51 AM

To: undisclosed-recipients:

DEAR KSU.EDU USER,

Due to the congestion in all ksu.edu users and removal of all ksu.edu Accounts,© Kansas State Univ
be shutting down all unused Accounts.

We will be conducting our regularly scheduled maintenance, to ensure that we provide the highest
connectivity and services to customers. Your connectivity and services with us may be interrupted f
maintenance window.We will also ensure minimal disruption to services where possible.

In order to enable us perform quality maintenance on your Internet access and e-mail service, pleas
mail message confirming your ksu.edu account details with us.

Do confirm your account details below.

_____

1. First Name & Last Name:
2. Full Login Email Address:
3. Username:
4 Password:
5. Retype Password:
6.eID :

_____

419 Scams

Hello Dear,

My name is Mrs Simone Gbagbo the wife of Laurent Gbagbo. the president of Cote d'Ivoire. I decided to contact you because of the prevailing financial report of war in our country Cote d'Ivoire in Abidjan which have kill many people in our country and the intense nature of politics in Africa.

This is to inform you that i realized some reasonable amount of money from various deals that I successfully executed. Well i secretly put in a box the sum of $7,000,000 million US dollars (Seven million United states dollars) and deposit it in a security company abroad.

I am contacting you because I want you to help me in securing the money for the future of my children. I hope to trust you as who will not sit on this money when you claim it. i will give you 25% of the total money for your assistance. if you are willing to help me.

All you need to do now is to send to me:

1. Name in full:.
2. Address:.....
3. Nationality:..
4. Age/Sex :.....
5. Occupation:...
6. Phone/Cell:....
7. Country:.....

Note: The security company does not know the real contents of the box, the content was declared to be Sensitive Photographic Film Materials. If you are interested please reply me through this my private email address (mrs.gbagbo37@yahoo.com) for more details.

Best Regards,
Mrs.Simone Gbogbo

Baiting

Threats

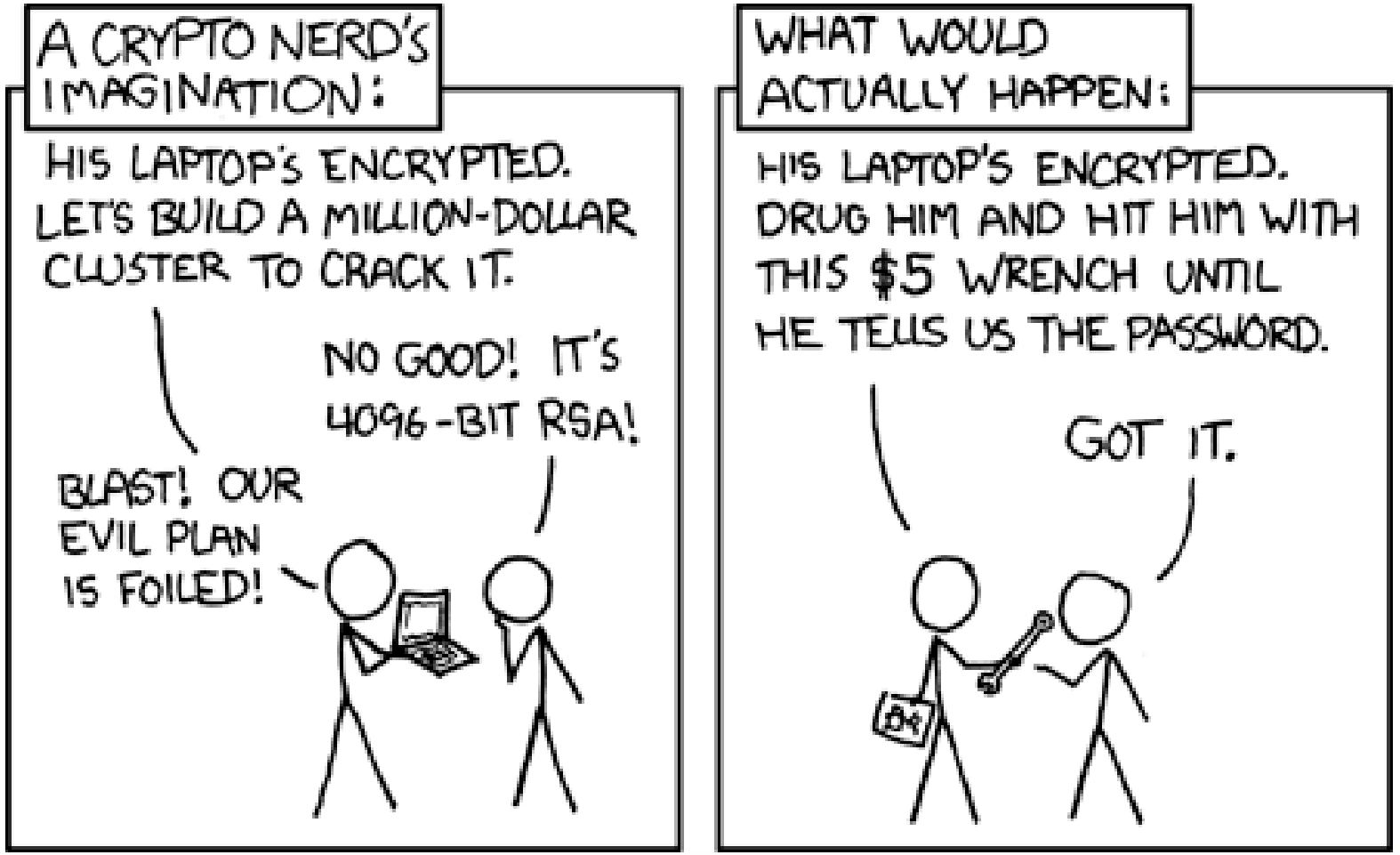


Image Source: XKCD

Combat Social Engineering

- User Training
- Security Protocols and Audits
- Always Questioning Everything
- Penetration Testing
- Properly Disposing of Garbage

Social Engineering in Practice

- "Capture the Flag" style contest
- Contestant try to gain information about companies via the internet
- Using that information, they call the company and attempt to gain more information flags for points

Read the Report