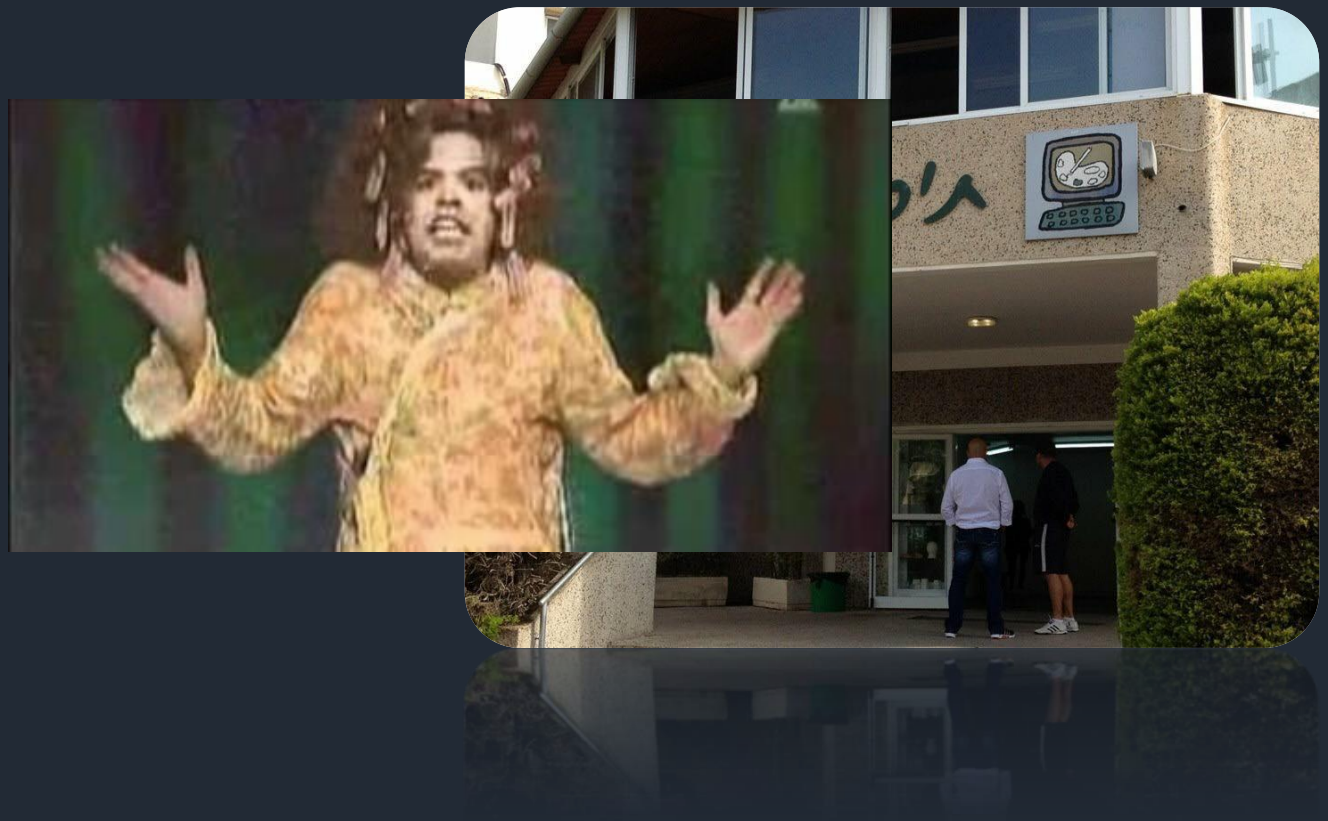
Usability and Psychology

Or

- Why the user is just as BIG of a vulnerability, as the code -

What we will talk about

קישור



But why?

- Many real attacks exploit psychology at least as much as technology
- We've evolved psychological tools over millions of years, to help us deal with deception in face-to-face context
- People are getting better at technology

Pretexting

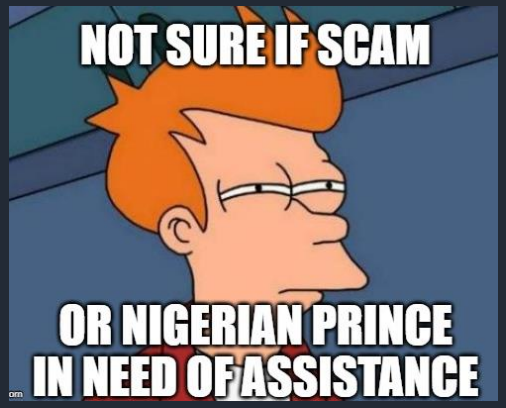
- Retrieving information using a third party
  The target -> Staff
- Most people will not consider the information as critical or just won't care
- As simple as a phone call – Israeli scam

Phishing

- Pretending to be a trusted entity
  The target -> customers

- Attacks against banks started in 2003, but were greedy and obvious.
  Nowadays, they are much more tricky.

- What's so tricky?

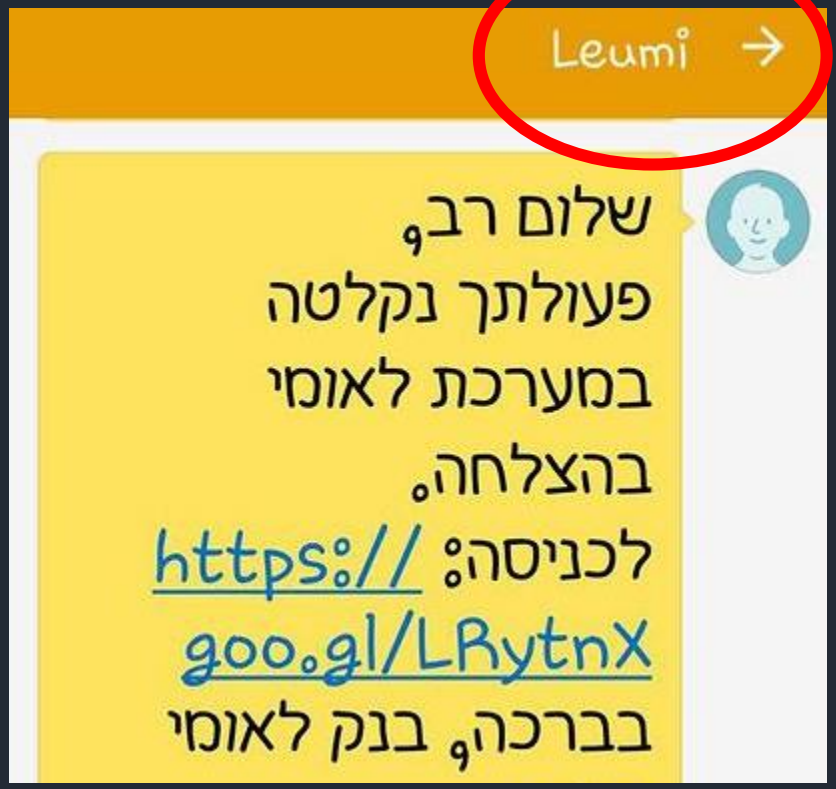


Pretexting
Phising
Passwords
Design
CAPTCHA
Future
Recap

- Aoccdrnig to a rscheearch at Cmabrigde Uinervtisy, it deosn't mttaer in waht oredr the ltteers in a wrod are, the olny iprmoetnt tihng is taht the frist and lsat ltteer be at the rghit pclae.

  The rset can be a toatl mses and you can sitll raed it wouthit porbelm. Tihs is bcuseae the huamn mnid deos not raed ervey lteter by istlef, but the wrod as a wlohe.

מקור



מקור

מקור

plications Places System
Isr
בנק ... | PHP... | Wel... | Goo... | מח... | נענע... | Nik... | חיבו... | המו... | Fac... | New T
81-86-54-21.dsl.pipex.com/www.bankhapoalim.co.il/
Google Reader | ynet | Facebook | אינטרנט ישראל | URL Decoder/Enc...

שכחת סיסמתך? כניסה

הצטרפות לפועלים באינטרנט

- אחריות ואבטחת מידע
- סרטון הדגמה למשתמש חדש
- הטבות בפועלים באינטרנט

אפליקציית הארנק הסלולרי

מהיום, ה-iPhone שלכם מחליף את הארנק!

להורדה חינם מ-AppStore

מעוניין לפתוח חשבון בבנק הפועלים?

פתח חשבון עכשיו

כדאי לדעת

- פעילים - סקירה כלכלית לחודש אוקטובר
- סימולטור אסטרטגיות מעו"ף - להתאמן, ללמוד ולהכיר את עולם המעו"ף מקרוב

פועלים באינטרנט בשוק ההון | Twitter | Widget | סקירות ותחזיות

תל אביב | חו"ל

נכון ל: 21.10.10 16:26

ת"א 25	1272.25	1.24%
ת"א 100	1172.9	1.05%
תל-טק 15	231.5	1.08%

תל אביב 25 ■ תל אביב 100 ■ לפורטל הפיננסי

מט"ח

דולר יציג	21.10.10	3.610
אירו יציג	21.10.10	5.064
ריבית פריים		3.5%

לשערים נוספים

ערוצי שירות
סניפים
אינטרנט
טלפון
סלולרי
אייפון

לקוחות
בנקאות פרטית
סטודנטים
חיילים
צעירים
דן חסכן

מוצרים ושירותים
יתרון מובנה
פיקדונות
תוכניות חיסכון
אימות פרויקט בבנייה
הלוואות

עוד בפועלים
משכנתא
פועלים אקספרס
פעילים
ישראכרט

הבנק ופעילותו
אודות הבנק
אחריות חברתית
פועלים בקהילה
דרושים

עוד באתר
מפת אתר
תעריפון הבנק
מחשבונים
Newsletter
RSS

מקור

Phishing

- Pretending to be a trusted entity
  The target -> customers
- Attacks against banks started in 2003, but were greedy and obvious.
  Nowadays, they are much more tricky.
- What's so tricky?
- The target -> customers
  Hence much harder to deal with.

Passwords

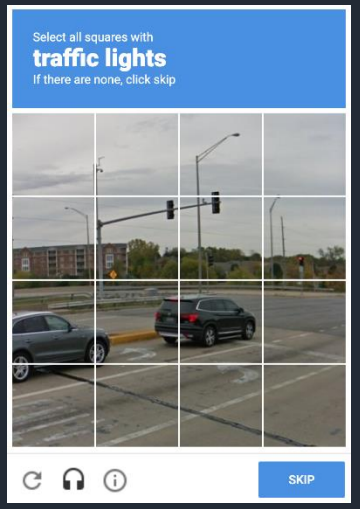
- One of the biggest practical problems facing security engineers today
- Reliable password entry
- Remembering the password
- Naive password choice

Design Errors

- Easy-to-guess security questions
- Using the same credential as both the “Key” and the “Hint”

CAPTCHAs

- Completely Automated Public Turing Test To Tell Computers and Humans Apart
- Trying to use the brain's strengths, rather than its weaknesses
- Getting more and more complex for computers, but not the brain
- Bypass by using more brains

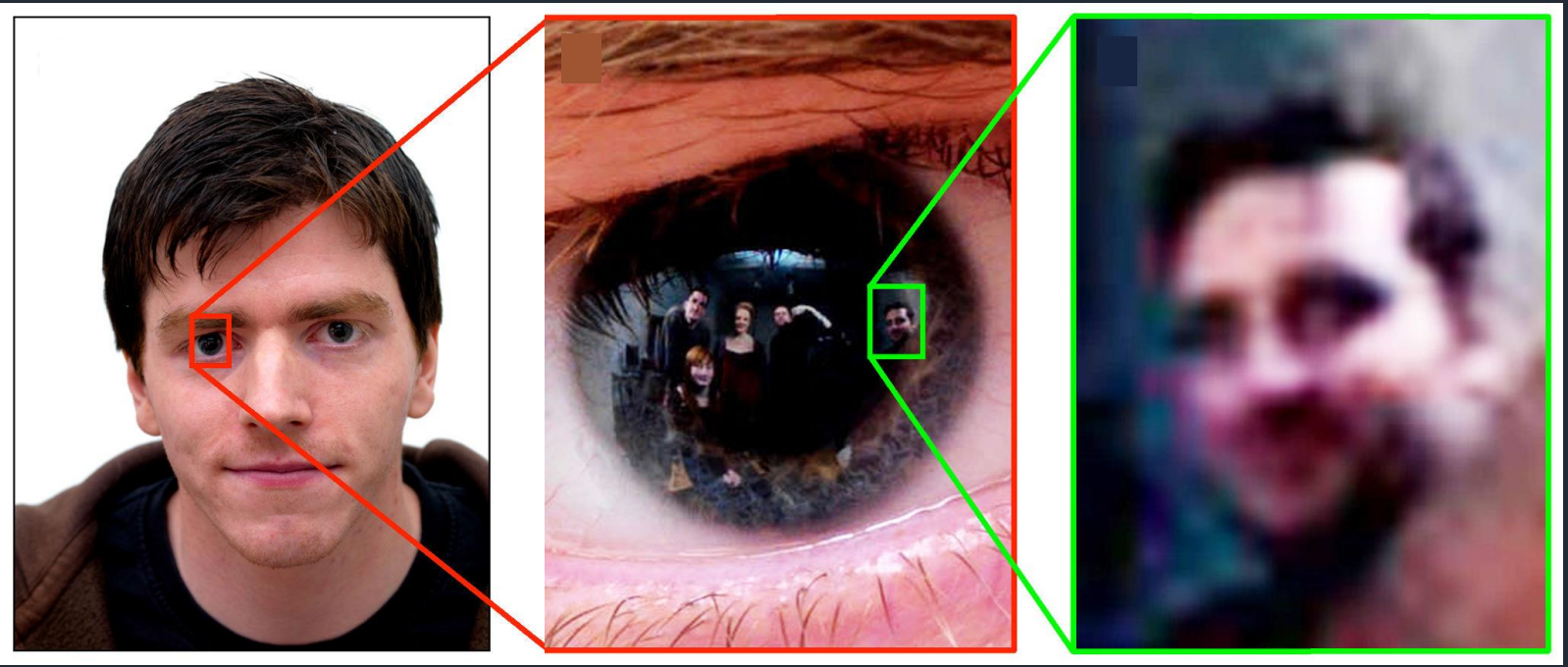


מקור

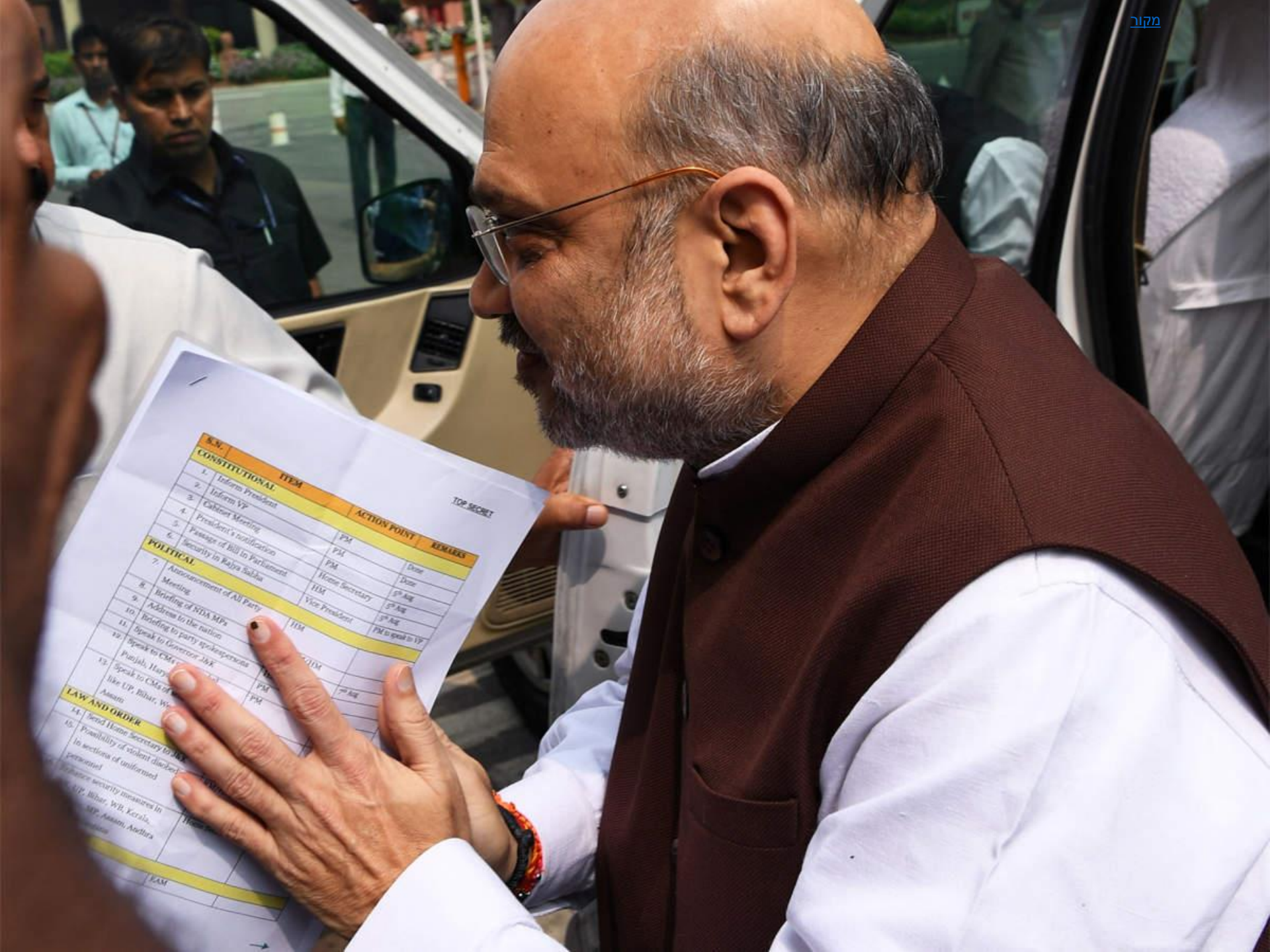
The future of phising?

- Targeted and changing content, similar to ads and spam.
- Using common requests or public data for phishing.

מקור



מקור


TOP SECRET
S.N.
ITEM
ACTION POINT
REMARKS
CONSTITUTIONAL
1. Inform President
2. Inform VP
3. Cabinet Meeting
4. President's notification
5. Passage of Bill in Parliament
6. Security in Rajya Sabha
POLITICAL
7. Announcement of All Party Meeting
8. Briefing of NDA MPs
9. Address to the nation
10. Briefing to party spokespersons
11. Speak to Governor J&K
12. Speak to CMs of Punjab, Haryana
13. Speak to CMs of like UP, Bihar, W Assam
LAW AND ORDER
14. Send Home Secretary to J&K
15. Possibility of violent disorder in sections of uniformed personnel
Enhance security measures in UP, Bihar, WB, Kerala, MP, Assam, Andhra
PM
HM
Home Secretary
Vice President
Done
Done
5th Aug
5th Aug
5th Aug
PM to speak to VP

מקור

Let's sum it up

- Pretexting
- Phishing
- Passwords
- CAPTCHAs
- Think ahead – what could be used next?

But…

- What about Raya?

- Thank you for listening -