

# 2550 Intro to cybersecurity

## L12: social engineering

abhi shelat

Thanks to Ran

Lets do some class exercises in Q1.

A CRYPTO NERD'S  
IMAGINATION:

HIS LAPTOP'S ENCRYPTED.  
LET'S BUILD A MILLION-DOLLAR  
CLUSTER TO CRACK IT.

NO GOOD! IT'S  
4096-BIT RSA!

BLAST! OUR  
EVIL PLAN  
IS FOILED!



WHAT WOULD  
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.  
DRUG HIM AND HIT HIM WITH  
THIS \$5 WRENCH UNTIL  
HE TELLS US THE PASSWORD.

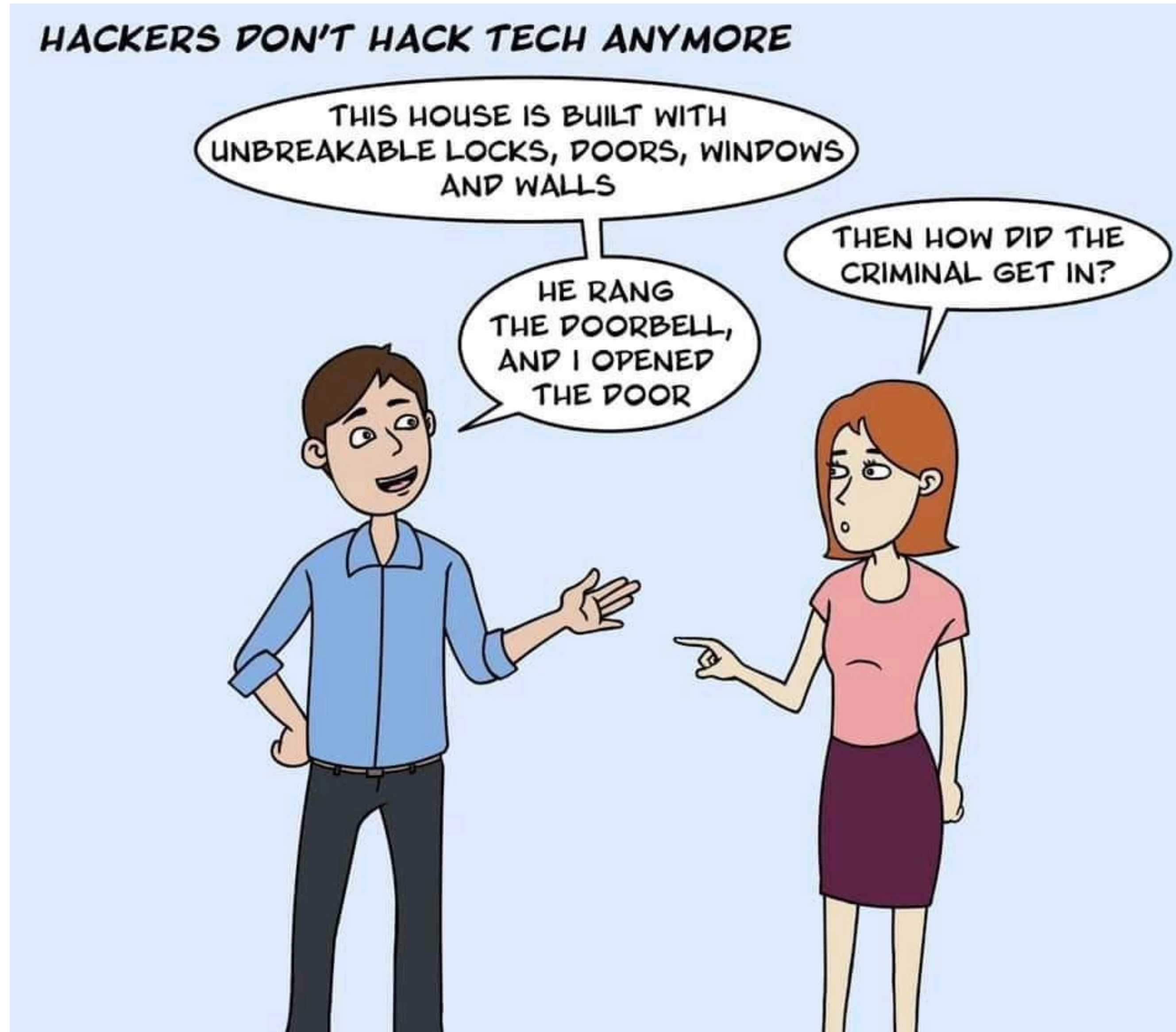


## HACKERS DON'T HACK TECH ANYMORE

THIS HOUSE IS BUILT WITH  
UNBREAKABLE LOCKS, DOORS, WINDOWS  
AND WALLS

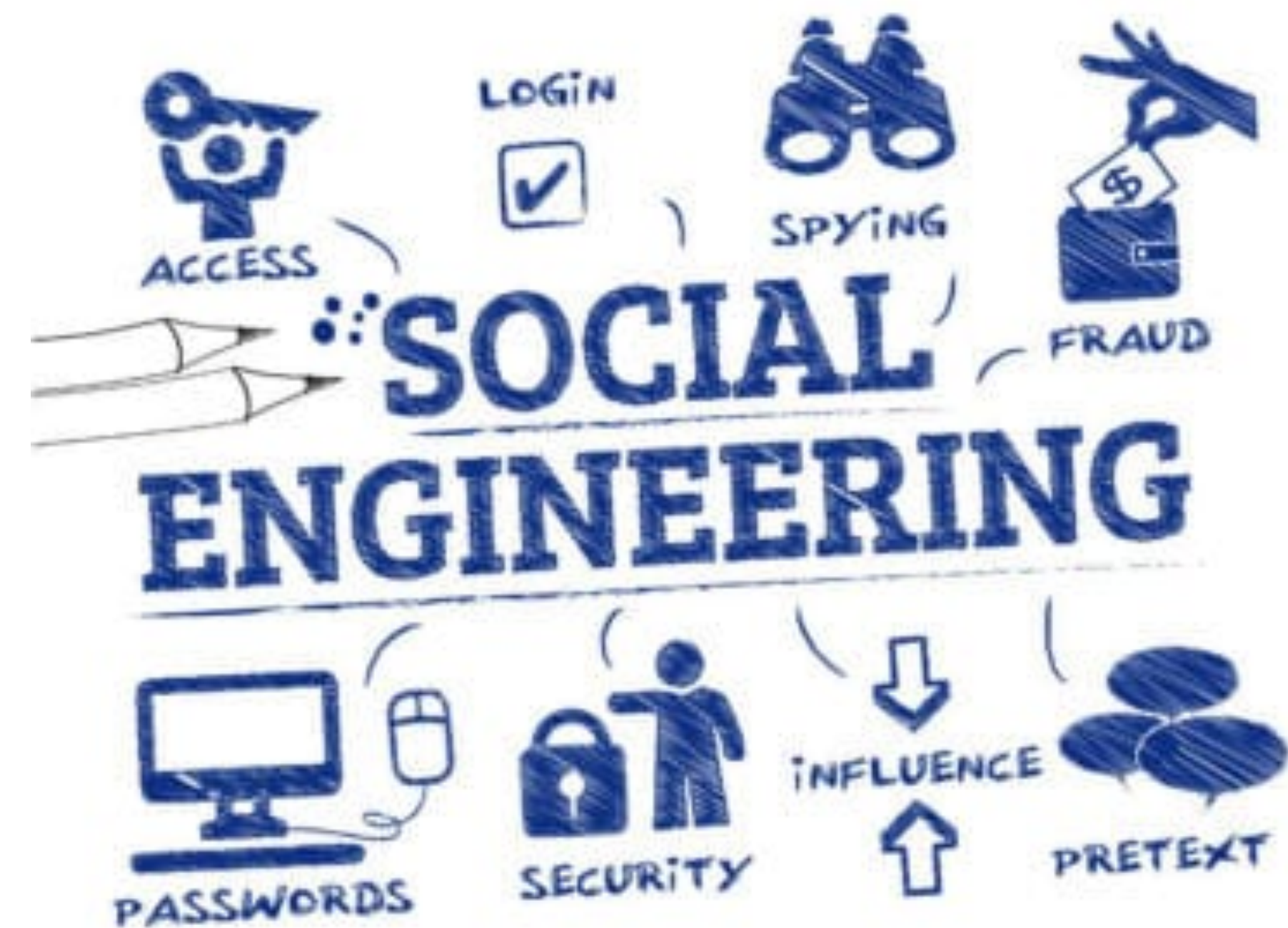
HE RANG  
THE DOORBELL,  
AND I OPENED  
THE DOOR

THEN HOW DID THE  
CRIMINAL GET IN?



# Social Engineering

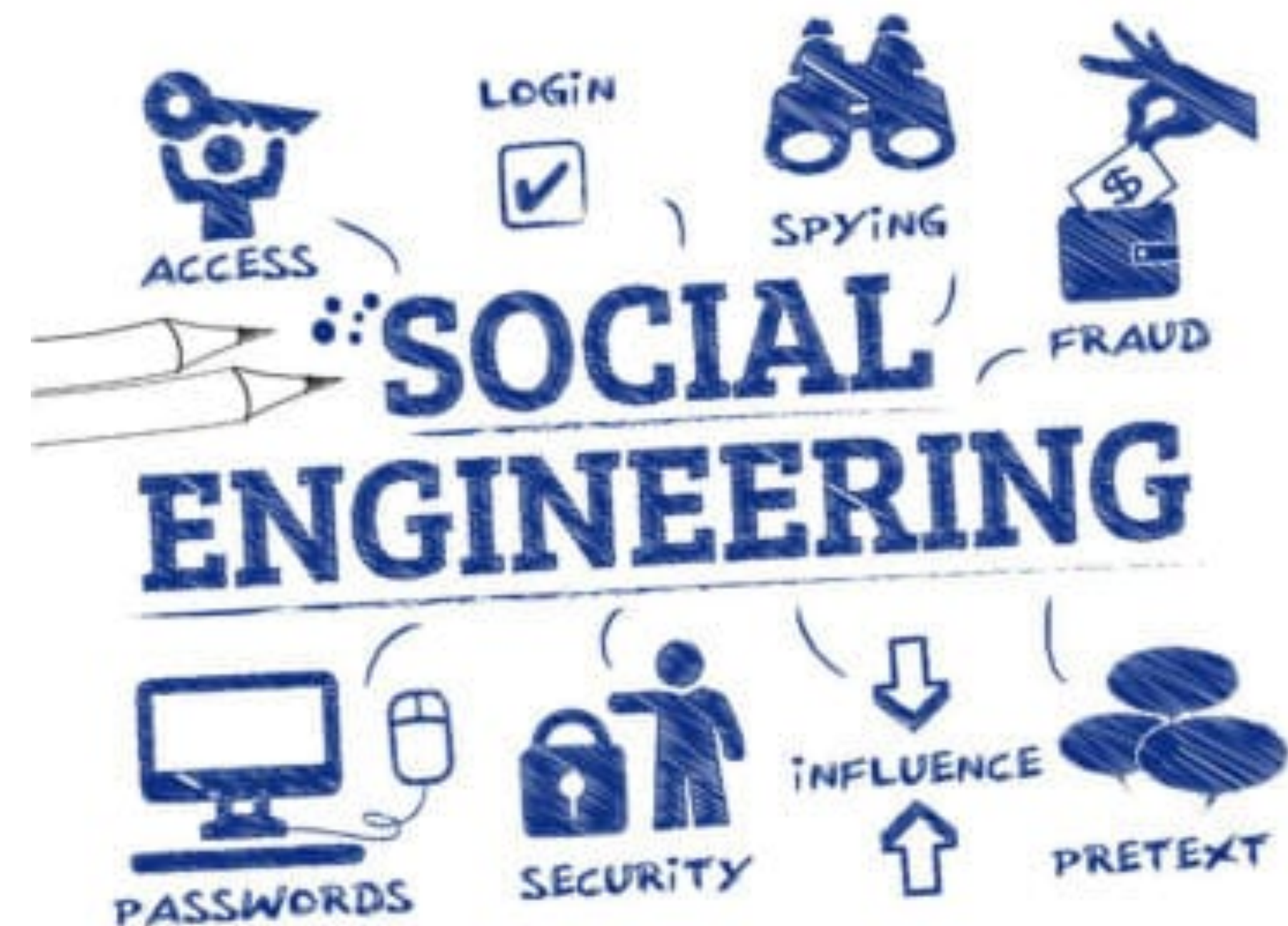
[https://www.youtube.com/watch?v=UzvPP6\\_LRHc](https://www.youtube.com/watch?v=UzvPP6_LRHc)



<https://>

# Social Engineering

A term used for a broad range of malicious activities accomplished through human interactions



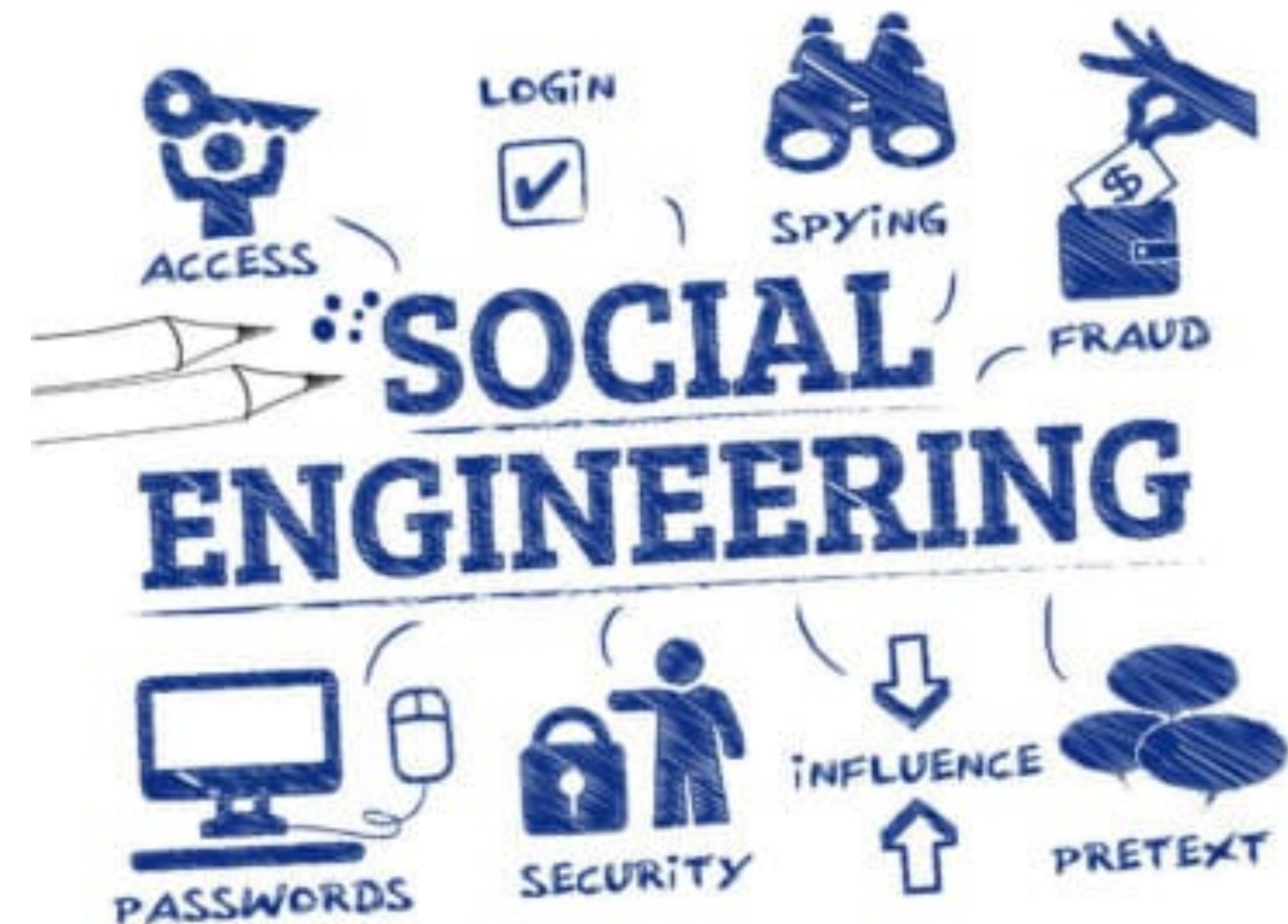
[https://www.youtube.com/watch?v=UzvPP6\\_LRHc](https://www.youtube.com/watch?v=UzvPP6_LRHc)

<https://>

# Social Engineering

A term used for a broad range of malicious activities accomplished through human interactions

Mainly using psychological manipulation to trick users into making security mistakes



[https://www.youtube.com/watch?v=UzvPP6\\_LRHc](https://www.youtube.com/watch?v=UzvPP6_LRHc)

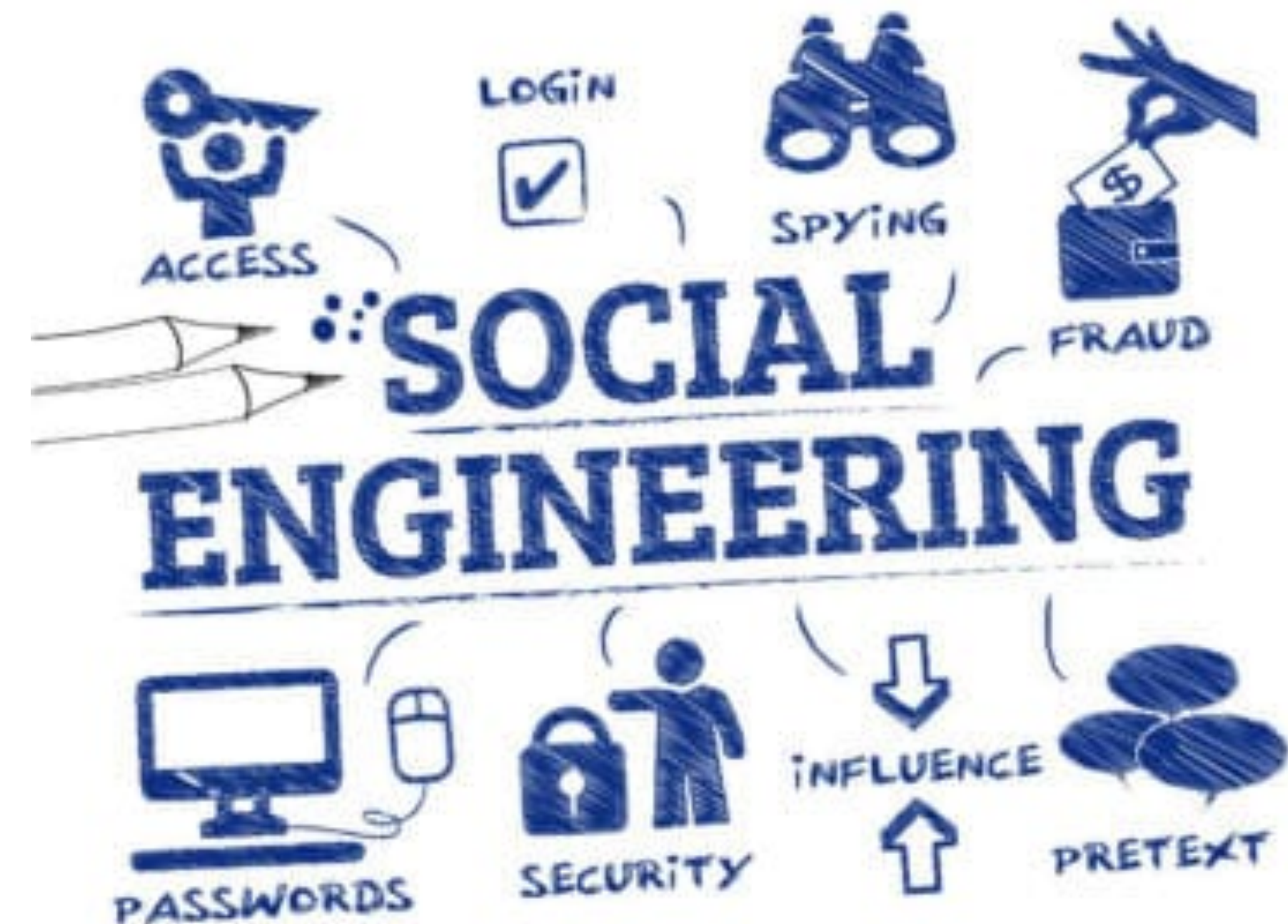
<https://>

# Social Engineering

A term used for a broad range of malicious activities accomplished through human interactions

Mainly using psychological manipulation to trick users into making security mistakes

- Disclose confidential/sensitive information



[https://www.youtube.com/watch?v=UzvPP6\\_LRHc](https://www.youtube.com/watch?v=UzvPP6_LRHc)

<https://>



# Social Engineering

A term used for a broad range of malicious activities accomplished through human interactions

Mainly using psychological manipulation to trick users into making security mistakes

- Disclose confidential/sensitive information
- Transfer money



[https://www.youtube.com/watch?v=UzvPP6\\_LRHc](https://www.youtube.com/watch?v=UzvPP6_LRHc)

<https://>

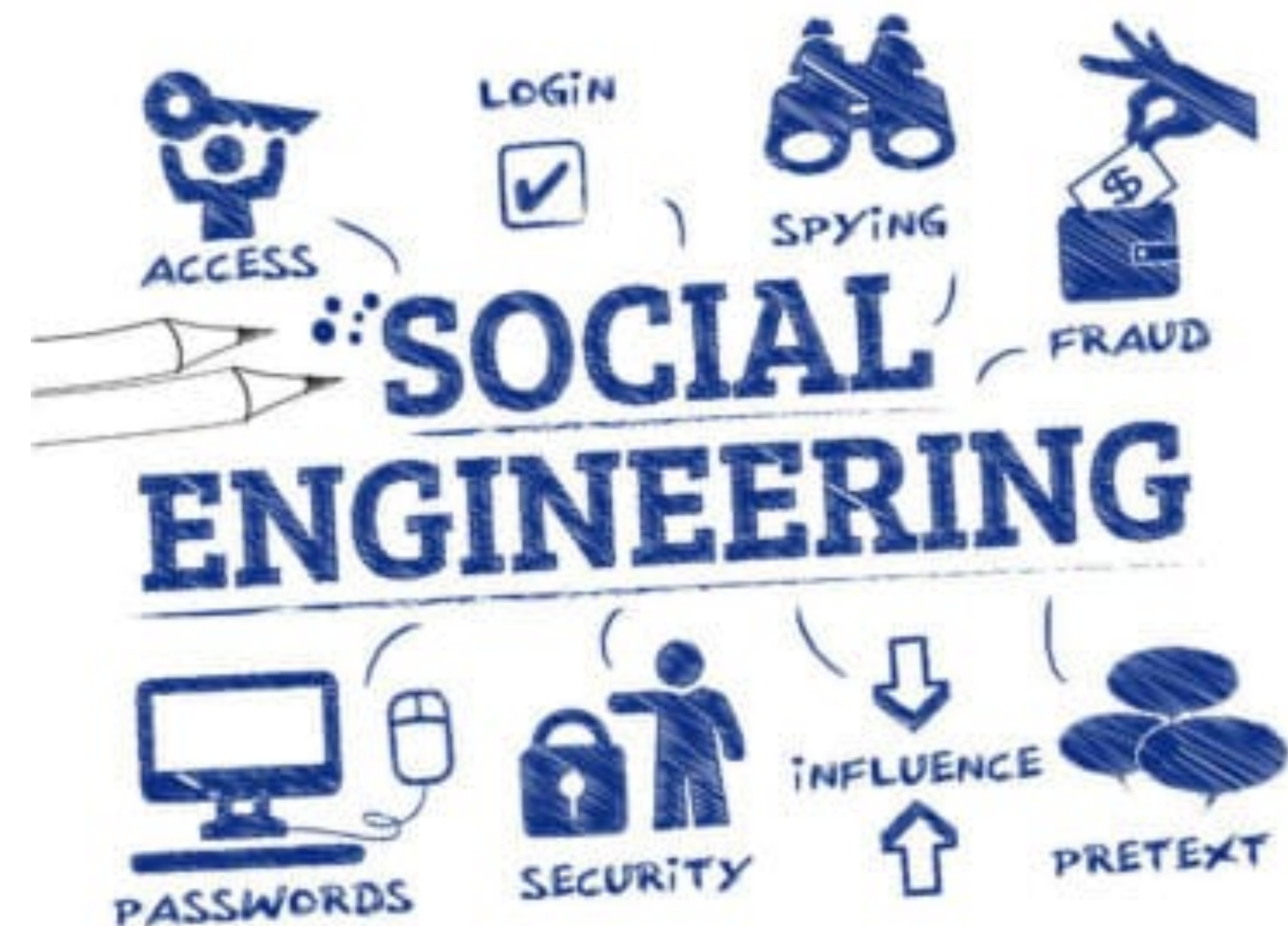
# Social Engineering

A term used for a broad range of malicious activities accomplished through human interactions

Mainly using psychological manipulation to trick users into making security mistakes

- Disclose confidential/sensitive information
- Transfer money
- Enable access to restricted systems

[https://www.youtube.com/watch?v=UzvPP6\\_LRHc](https://www.youtube.com/watch?v=UzvPP6_LRHc)



<https://>

# Social Engineering

A term used for a broad range of malicious activities accomplished through human interactions

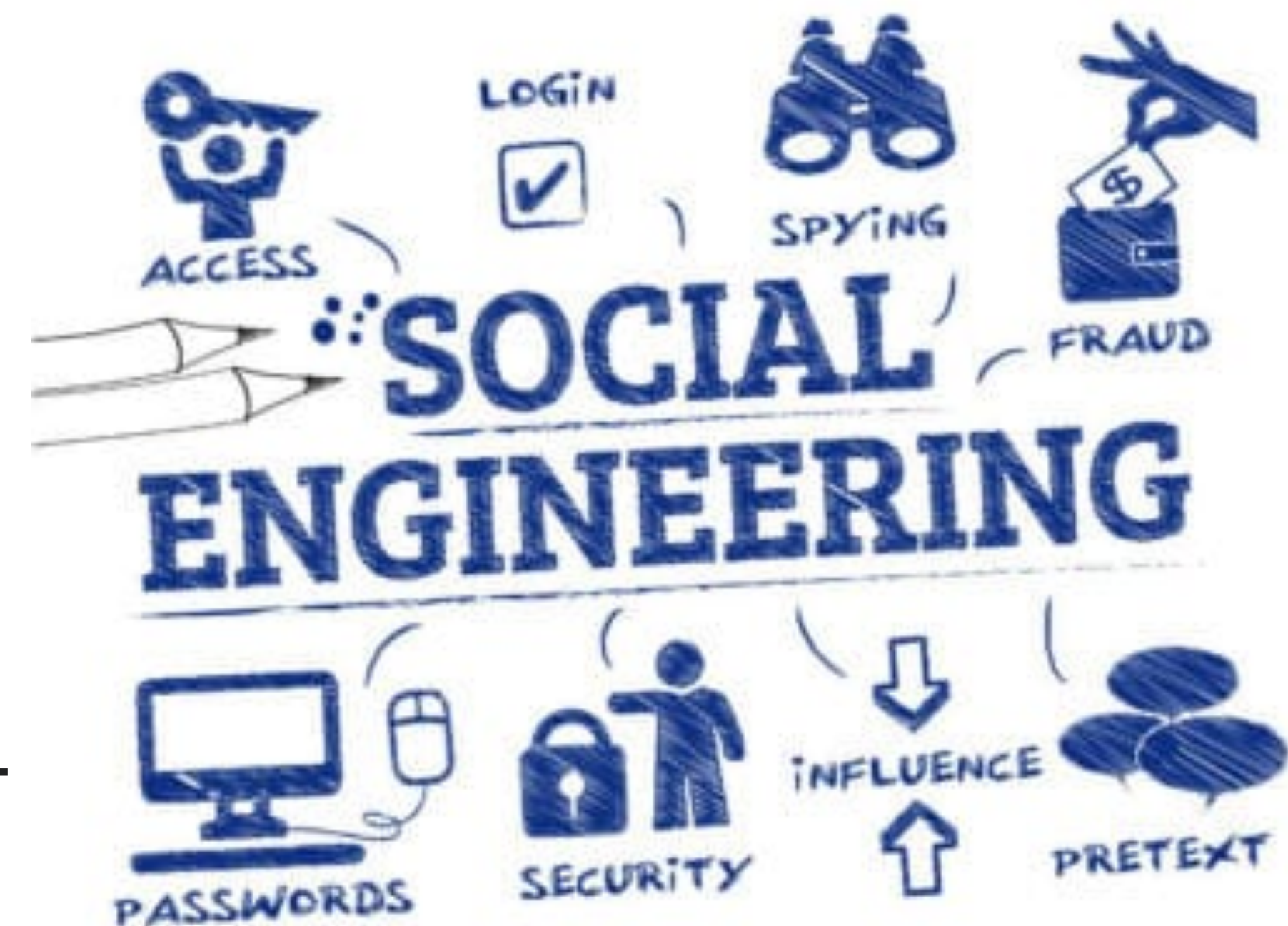
Mainly using psychological manipulation to trick users into making security mistakes

- Disclose confidential/sensitive information
- Transfer money
- Enable access to restricted systems

Demonstration from Jimmy Kimmel

<https://www.youtube.com/watch?v=opRMrEfAlil>

[https://www.youtube.com/watch?v=UzvPP6\\_LRHc](https://www.youtube.com/watch?v=UzvPP6_LRHc)



<https://>

# Social Engineering 100yrs ago

# Social Engineering 100yrs ago

In 1906 Friedrich Wilhelm Voigt, a shoemaker,



# Social Engineering 100yrs ago

- In 1906 Friedrich Wilhelm Voigt, a shoemaker,
- Purchased a used military officer uniform



# Social Engineering 100yrs ago

In 1906 Friedrich Wilhelm Voigt, a shoemaker,

- Purchased a used military officer uniform
- Gathered 10 soldiers and took a train to Köpenick



# Social Engineering 100yrs ago

In 1906 Friedrich Wilhelm Voigt, a shoemaker,

- Purchased a used military officer uniform
- Gathered 10 soldiers and took a train to Köpenick
- Arrested the mayor and treasurer for crooked bookkeeping





# Social Engineering 100yrs ago

In 1906 Friedrich Wilhelm Voigt, a shoemaker,

- Purchased a used military officer uniform
- Gathered 10 soldiers and took a train to Köpenick
- Arrested the mayor and treasurer for crooked bookkeeping
- Confiscated 4000 marks (left a receipt)



# Social Engineering 100yrs ago

In 1906 Friedrich Wilhelm Voigt, a shoemaker,

- Purchased a used military officer uniform
- Gathered 10 soldiers and took a train to Köpenick
- Arrested the mayor and treasurer for crooked bookkeeping
- Confiscated 4000 marks (left a receipt)
- When the police came he had them serve coffee to the soldiers



# Social Engineering 100yrs ago

# Social Engineering 100yrs ago

In 1908 George C. Parker sold the Brooklyn bridge, several times



# Social Engineering 100yrs ago

In 1908 George C. Parker sold the Brooklyn bridge, several times

- Forged ownership documents



# Social Engineering 100yrs ago

In 1908 George C. Parker sold the Brooklyn bridge, several times

- Forged ownership documents
- Targeted newcomers to the 'land of opportunity'



# Social Engineering 100yrs ago

In 1908 George C. Parker sold the Brooklyn bridge, several times

- Forged ownership documents
- Targeted newcomers to the 'land of opportunity'
- Convinced buyers they could control access to the roadway



# Social Engineering 100yrs ago

In 1908 George C. Parker sold the Brooklyn bridge, several times

- Forged ownership documents
- Targeted newcomers to the 'land of opportunity'
- Convinced buyers they could control access to the roadway
- Buyers started collecting toll fees





# Social Engineering 100yrs ago

In 1908 George C. Parker sold the Brooklyn bridge, several times

- Forged ownership documents
- Targeted newcomers to the 'land of opportunity'
- Convinced buyers they could control access to the roadway
- Buyers started collecting toll fees
- Also sold the Statue of Liberty, ...



# Social Engineering 100yrs ago

# Social Engineering 100yrs ago

In 1925 Victor Lustig sold the Eiffel Tower, twice



<https://medium.com/>

# Social Engineering 100yrs ago

In 1925 Victor Lustig sold the Eiffel Tower, twice

- Read about the costly maintenance of the Eiffel tower



<https://medium.com/>

# Social Engineering 100yrs ago

In 1925 Victor Lustig sold the Eiffel Tower, twice

- Read about the costly maintenance of the Eiffel tower
- Impersonated as a legitimate authority



# Social Engineering 100yrs ago

In 1925 Victor Lustig sold the Eiffel Tower, twice

- Read about the costly maintenance of the Eiffel tower
- Impersonated as a legitimate authority
- Forged official documents



# Social Engineering 100yrs ago

In 1925 Victor Lustig sold the Eiffel Tower, twice

- Read about the costly maintenance of the Eiffel tower
- Impersonated as a legitimate authority
- Forged official documents
- Profiling: targeted his victim



# Social Engineering 100yrs ago

In 1925 Victor Lustig sold the Eiffel Tower, twice

- Read about the costly maintenance of the Eiffel tower
- Impersonated as a legitimate authority
- Forged official documents
- Profiling: targeted his victim
- Made an extremely good deal to the buyer

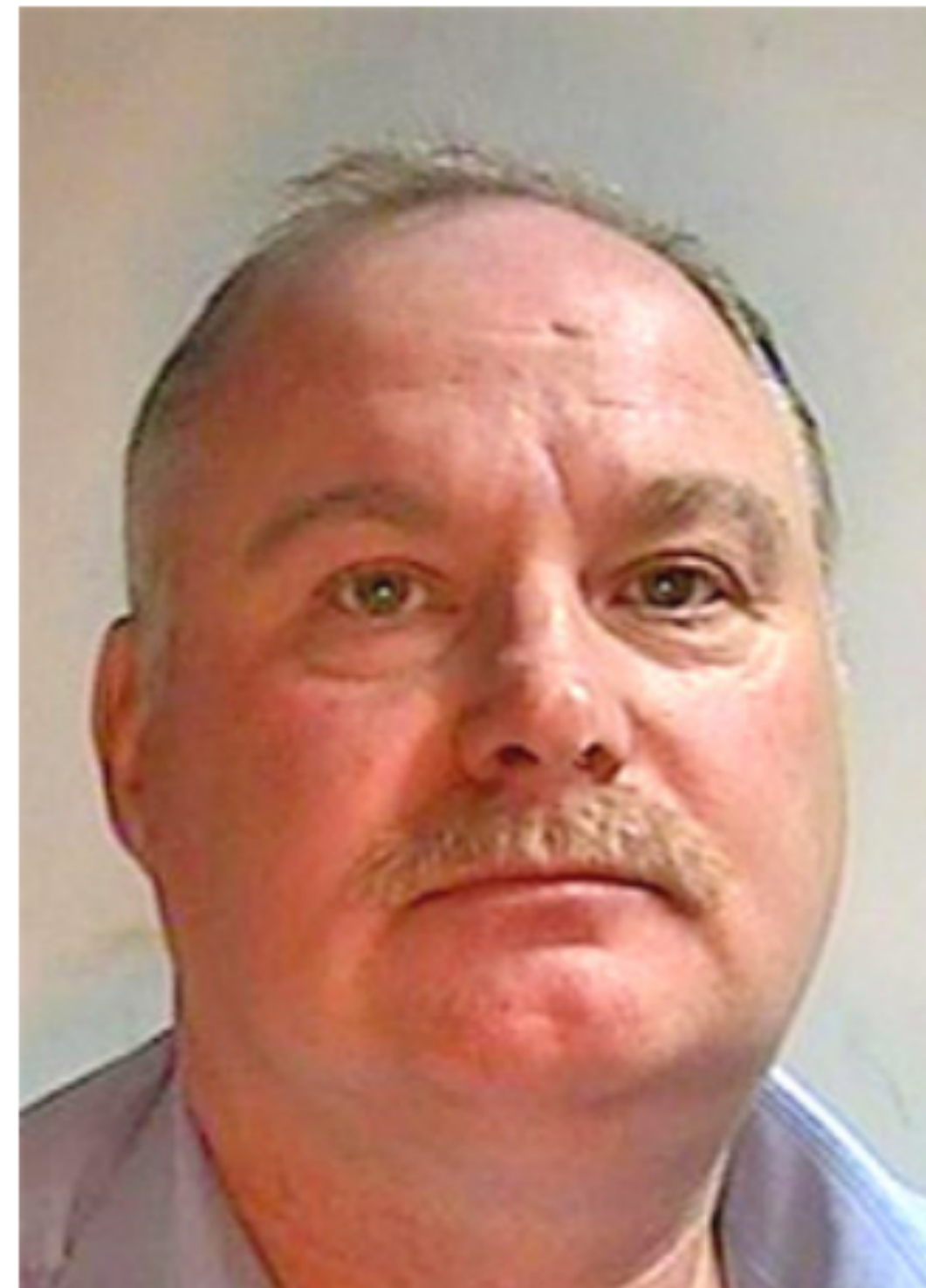




# The man who tried to sell the Ritz

When Anthony Lee offered buyers the hotel on the cheap, the deal looked too good to be true. It was — he didn't own it

By **Mark Hughes** | Wednesday 28 July 2010 00:00



Social Engineering 50yrs ago

# Social Engineering 50yrs ago

Frank Abagnale impersonations in the '60s



[https://  
en.wikip](https://en.wikipedia.org)

# Social Engineering 50yrs ago

Frank Abagnale impersonations in the '60s

- Airline pilot at Pan Am



[https://  
en.wikip](https://en.wikipedia.org)

# Social Engineering 50yrs ago

Frank Abagnale impersonations in the '60s

- Airline pilot at Pan Am
- TA at Brigham Young University



[https://  
en.wikip](https://en.wikipedia.org/wiki/Frank_Abagnale)

# Social Engineering 50yrs ago

## Frank Abagnale impersonations in the '60s

- Airline pilot at Pan Am
- TA at Brigham Young University
- Resident pediatrician in a Georgia hospital



[https://  
en.wikip](https://en.wikipedia.org)

# Social Engineering 50yrs ago

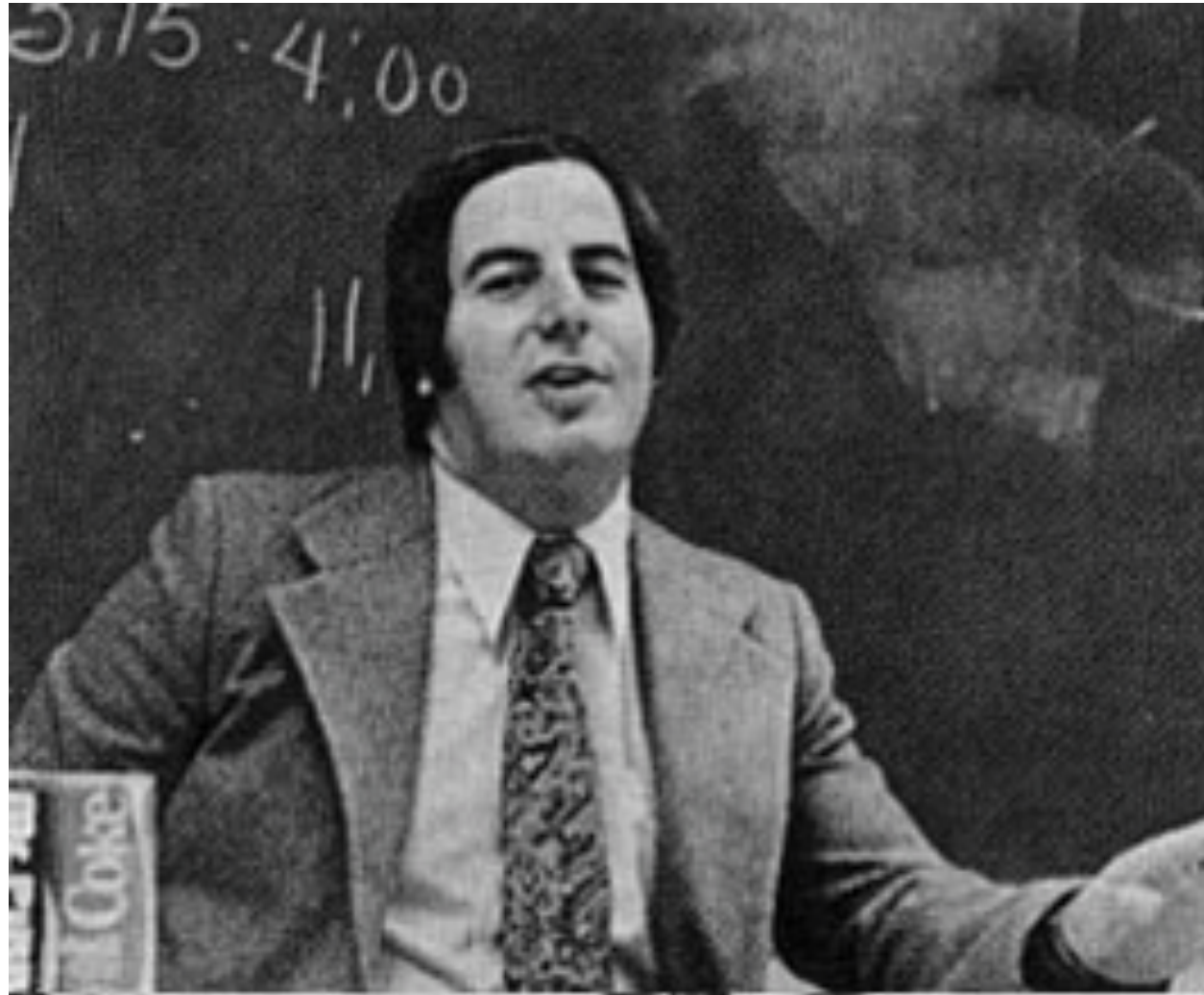
## Frank Abagnale impersonations in the '60s

- Airline pilot at Pan Am
- TA at Brigham Young University
- Resident pediatrician in a Georgia hospital
- Forged a Harvard University law transcript and worked at the Louisiana State Attorney General's office



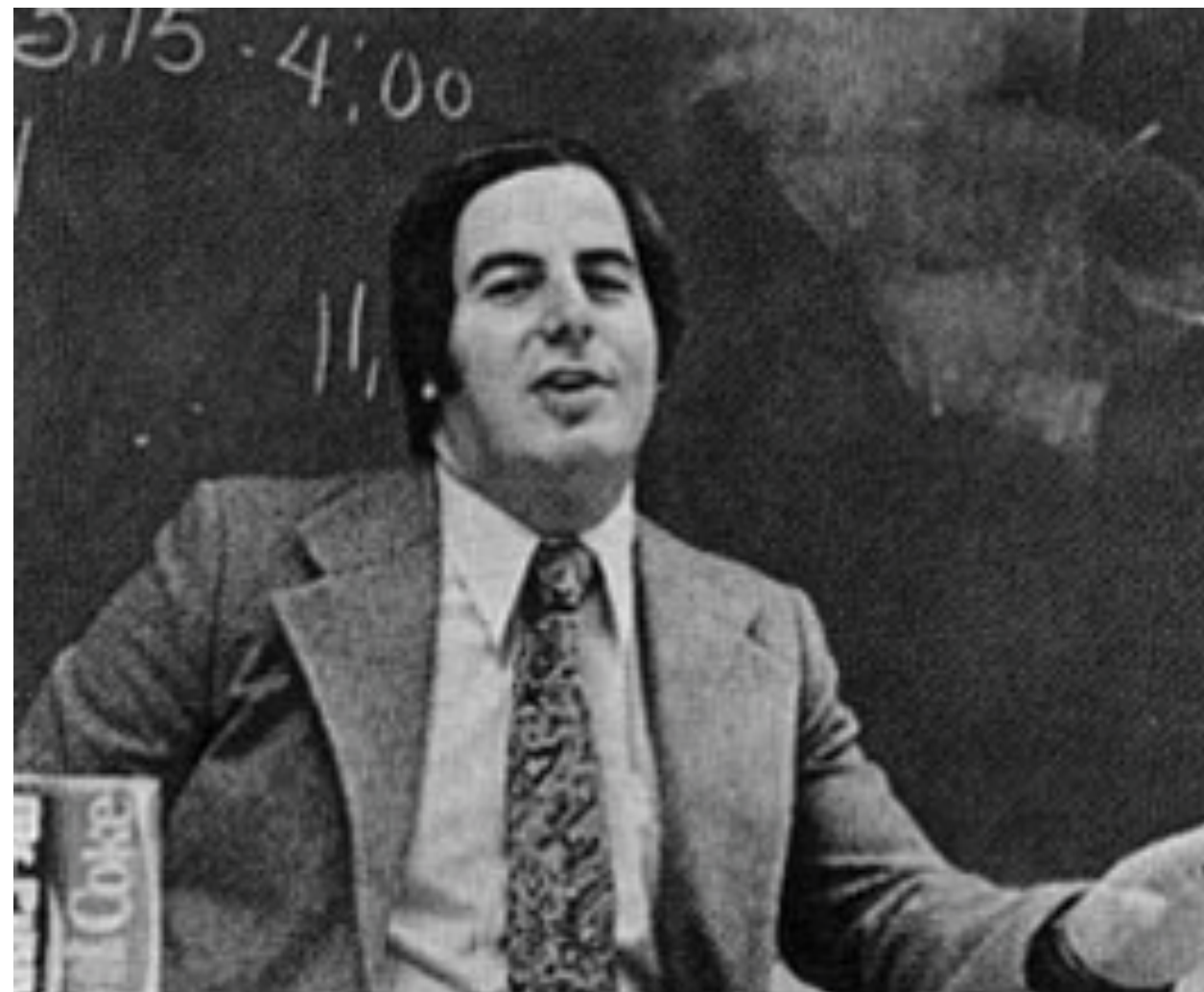
[https://  
en.wikip](https://en.wikipedia.org/wiki/Frank_Abagnale)

# Social Engineering 50yrs ago





# Social Engineering 50yrs ago



[https://  
en.wikip](https://en.wikipedia)

[www.taratara](http://www.taratara)

# Social Engineering 50yrs ago



leonardo dicaprio tom hanks



[www.taratara](http://www.taratara)

[en.wikip](http://en.wikipedia)

Social Engineering 50yrs ago

# Social Engineering 50yrs ago

## **Man arrested for impersonating pilot in Philadelphia**

**Nancy Trejos** USA TODAY

Published 10:38 a.m. ET Mar. 22, 2013 | Updated 11:03 a.m. ET Mar. 22, 2013

# Social Engineering 50yrs ago

## Man arrested for impersonating pilot in Philadelphia

**Nancy Trejos** USA TODAY

Published 10:38 a.m. ET Mar. 22, 2013 | Updated 11:03 a.m. ET Mar. 22, 2013

### Man arrested at Indian airport for impersonating Lufthansa pilot

Manveena Suri, CNN • Updated 21st November 2019



Social Engineering 30yrs ago

# Social Engineering 30yrs ago

Kevin Mitnick



# Social Engineering 30yrs ago

Kevin Mitnick

- Most famous hacker in '90s





# Social Engineering 30yrs ago

## Kevin Mitnick

- Most famous hacker in '90s
- Termed 'social engineering' in the context of IT security



# Social Engineering 30yrs ago

## Kevin Mitnick

- Most famous hacker in '90s
- Termed 'social engineering' in the context of IT security
- Known for hacking phone companies, Pacific Bell



# Social Engineering 30yrs ago

## Kevin Mitnick

- Most famous hacker in '90s
- Termed 'social engineering' in the context of IT security
- Known for hacking phone companies, Pacific Bell
- High-profile arrest in 1995

**WANTED**  
**BY U.S. MARSHALS**

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).  
United States Marshall Service NCIC entry number: (NOC/ W221440021 )

NAME: .....MITNICK, KEVIN DAVID  
AKS (S): .....MITNICK, KEVIN DAVID  
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: .....MALE  
Race: .....WHITE  
Place of Birth: .....VAN NUYS, CALIFORNIA  
Date(s) of Birth: .....08/06/63; 10/18/70  
Height: .....5'11"  
Weight: .....190  
Eyes: .....BLUE  
Hair: .....BROWN  
Skin tone: .....LIGHT



Social Engineering 20yrs ago

# Social Engineering 20yrs ago

ILOVEYOU worm



# Social Engineering 20yrs ago

## ILOVEYOU worm

- Spread via emails on May 4<sup>th</sup>, 2000



# Social Engineering 20yrs ago

## ILOVEYOU worm

- Spread via emails on May 4<sup>th</sup>, 2000
- Attachment: LOVE-LETTER-FOR-YOU.txt.vbs



# Social Engineering 20yrs ago

## ILOVEYOU worm

- Spread via emails on May 4<sup>th</sup>, 2000
- Attachment: LOVE-LETTER-FOR-YOU.txt.vbs
- vbs extension was hidden in Windows by default





# Social Engineering 20yrs ago

## ILOVEYOU worm

- Spread via emails on May 4<sup>th</sup>, 2000
- Attachment: LOVE-LETTER-FOR-YOU.txt.vbs
- vbs extension was hidden in Windows by default
- Considered as 1<sup>st</sup> socially engineered computer virus



# Social Engineering 20yrs ago

## ILOVEYOU worm

- Spread via emails on May 4<sup>th</sup>, 2000
- Attachment: LOVE-LETTER-FOR-YOU.txt.vbs
- vbs extension was hidden in Windows by default
- Considered as 1<sup>st</sup> socially engineered computer virus
- Overwrote files



# Social Engineering 20yrs ago

## ILOVEYOU worm

- Spread via emails on May 4<sup>th</sup>, 2000
- Attachment: LOVE-LETTER-FOR-YOU.txt.vbs
- vbs extension was hidden in Windows by default
- Considered as 1<sup>st</sup> socially engineered computer virus
- Overwrote files
- Spread to all contacts



# Social Engineering 20yrs ago

## ILOVEYOU worm

- Spread via emails on May 4<sup>th</sup>, 2000
- Attachment: LOVE-LETTER-FOR-YOU.txt.vbs
- vbs extension was hidden in Windows by default
- Considered as 1<sup>st</sup> socially engineered computer virus
- Overwrote files
- Spread to all contacts
- Infected 10% of connected computers



# Social Engineering 20yrs ago

## ILOVEYOU worm

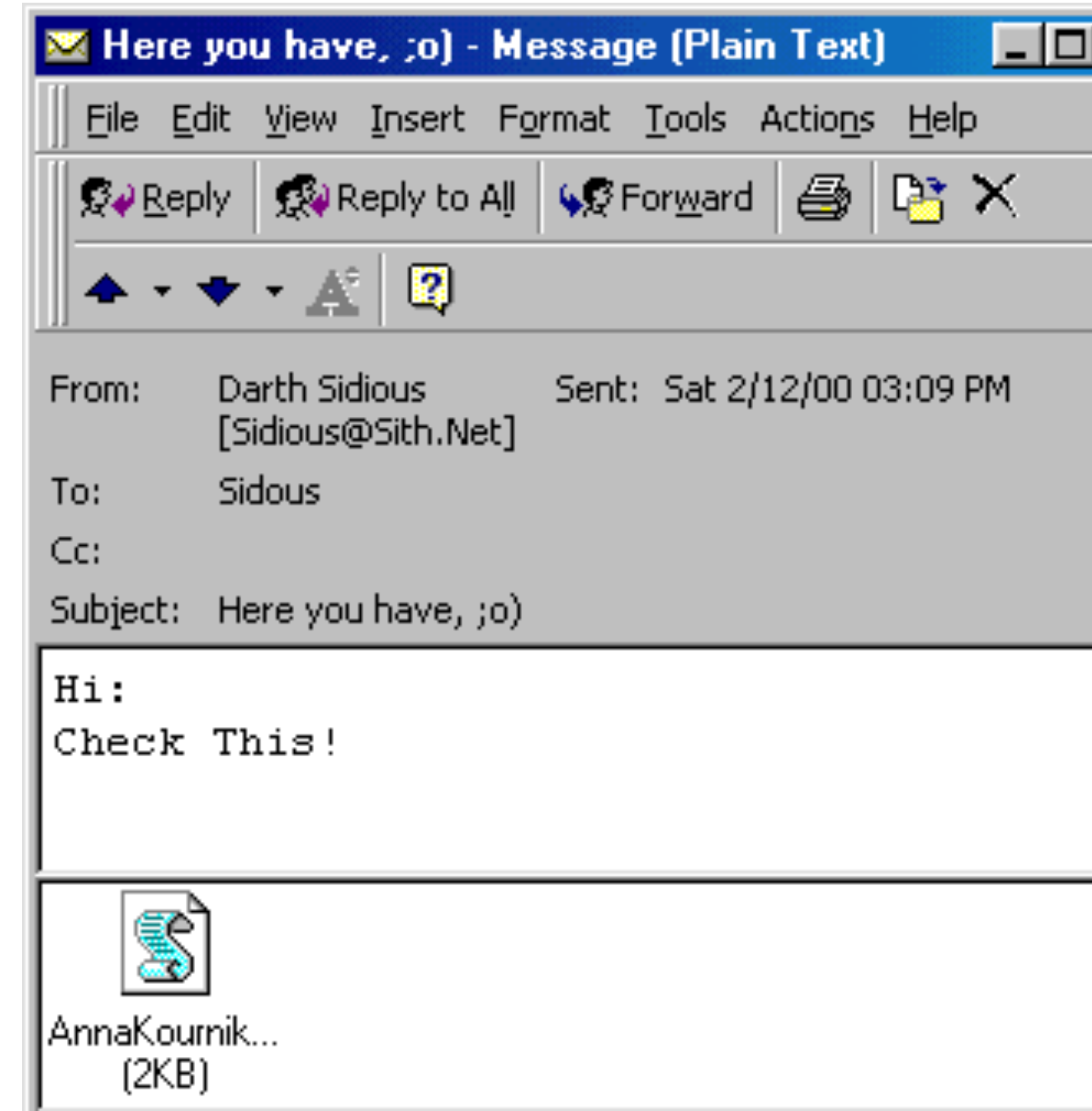
- Spread via emails on May 4<sup>th</sup>, 2000
- Attachment: LOVE-LETTER-FOR-YOU.txt.vbs
- vbs extension was hidden in Windows by default
- Considered as 1<sup>st</sup> socially engineered computer virus
- Overwrote files
- Spread to all contacts
- Infected 10% of connected computers
- Over \$5 billion damages



Social Engineering 20yrs ago

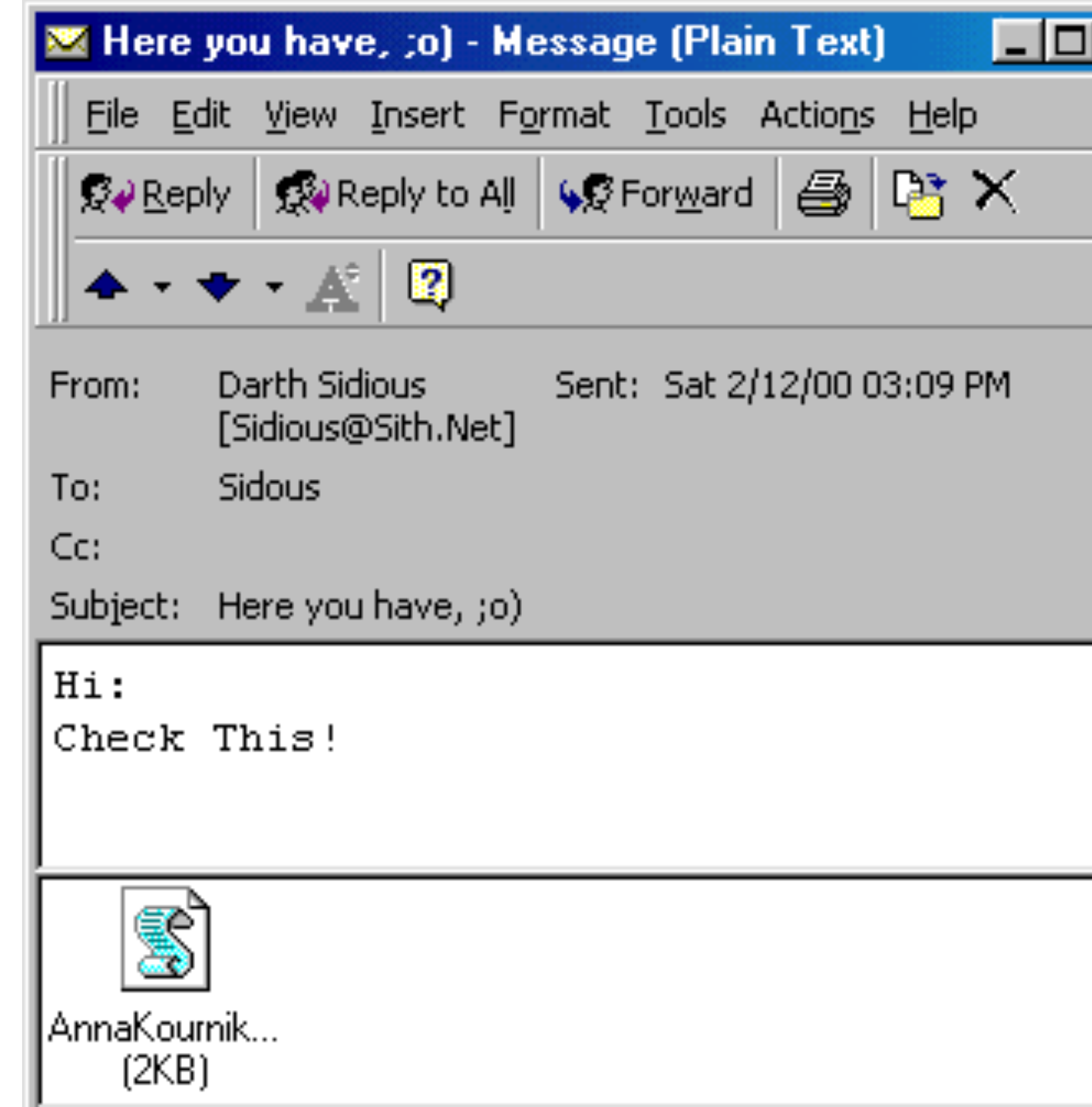
# Social Engineering 20yrs ago

## Anna Kournikova virus



# Social Engineering 20yrs ago

## Anna Kournikova virus

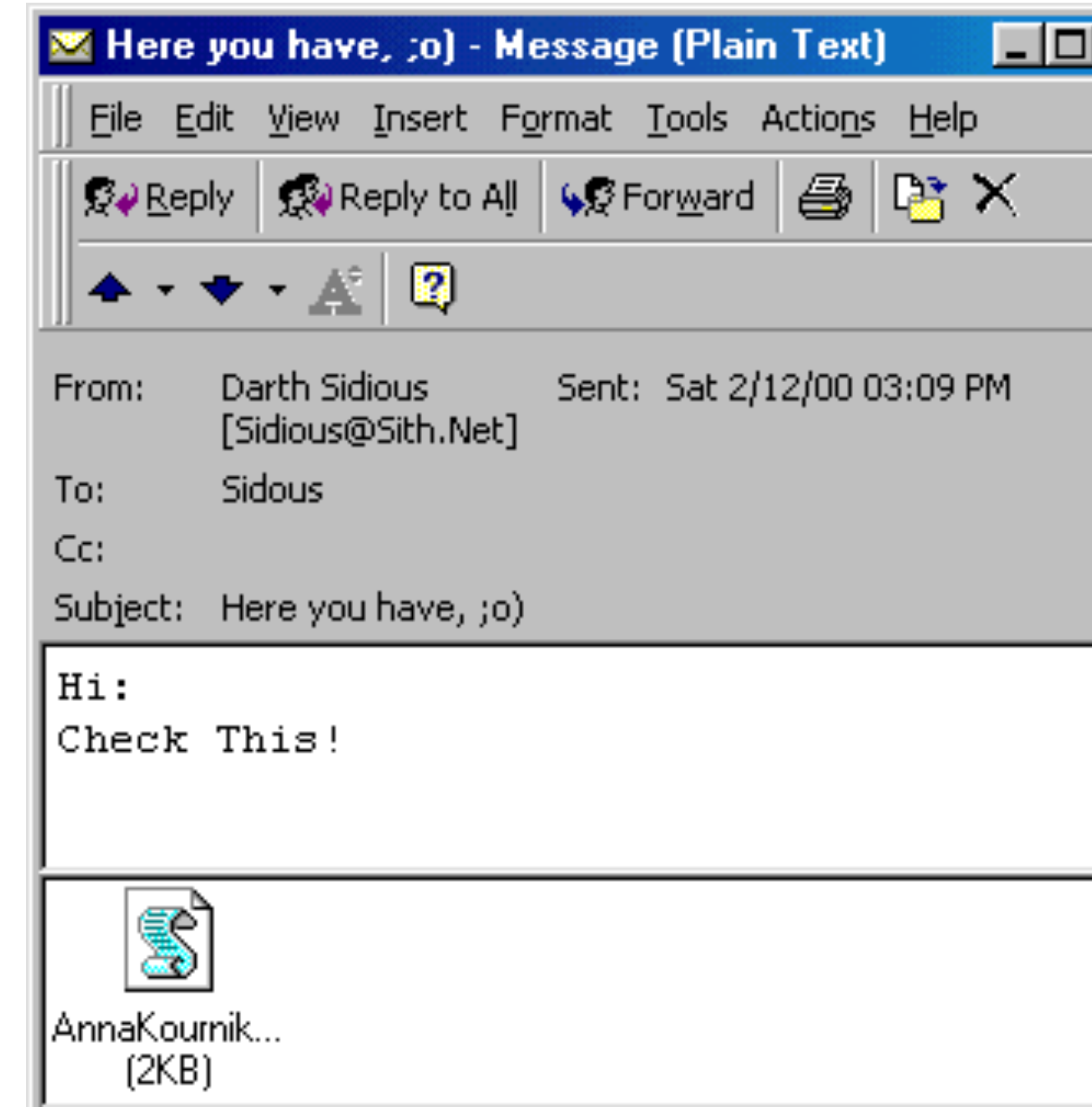




# Social Engineering 20yrs ago

## Anna Kournikova virus

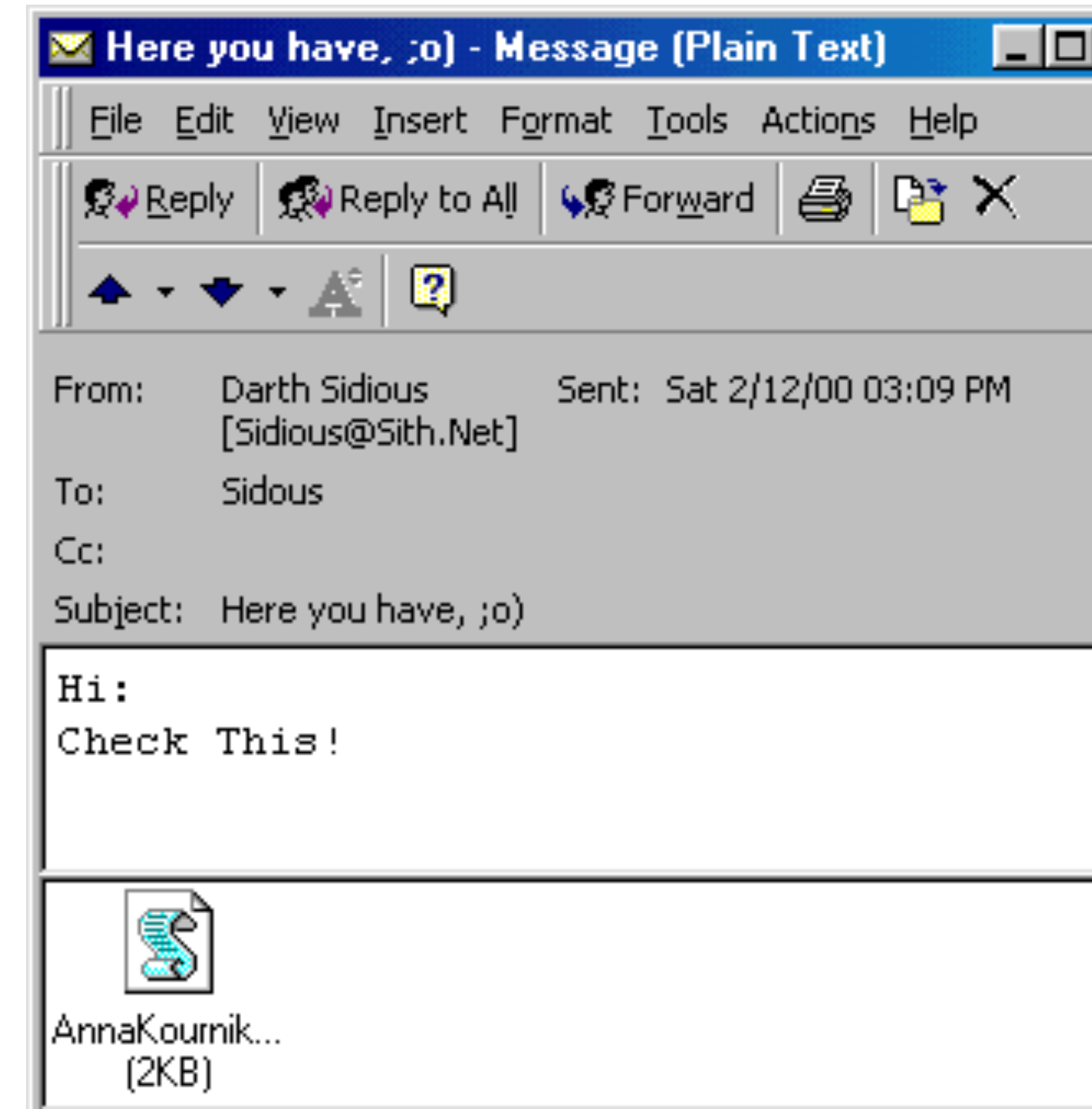
- Spread via emails on Feb 11<sup>th</sup>, 2001



# Social Engineering 20yrs ago

## Anna Kournikova virus

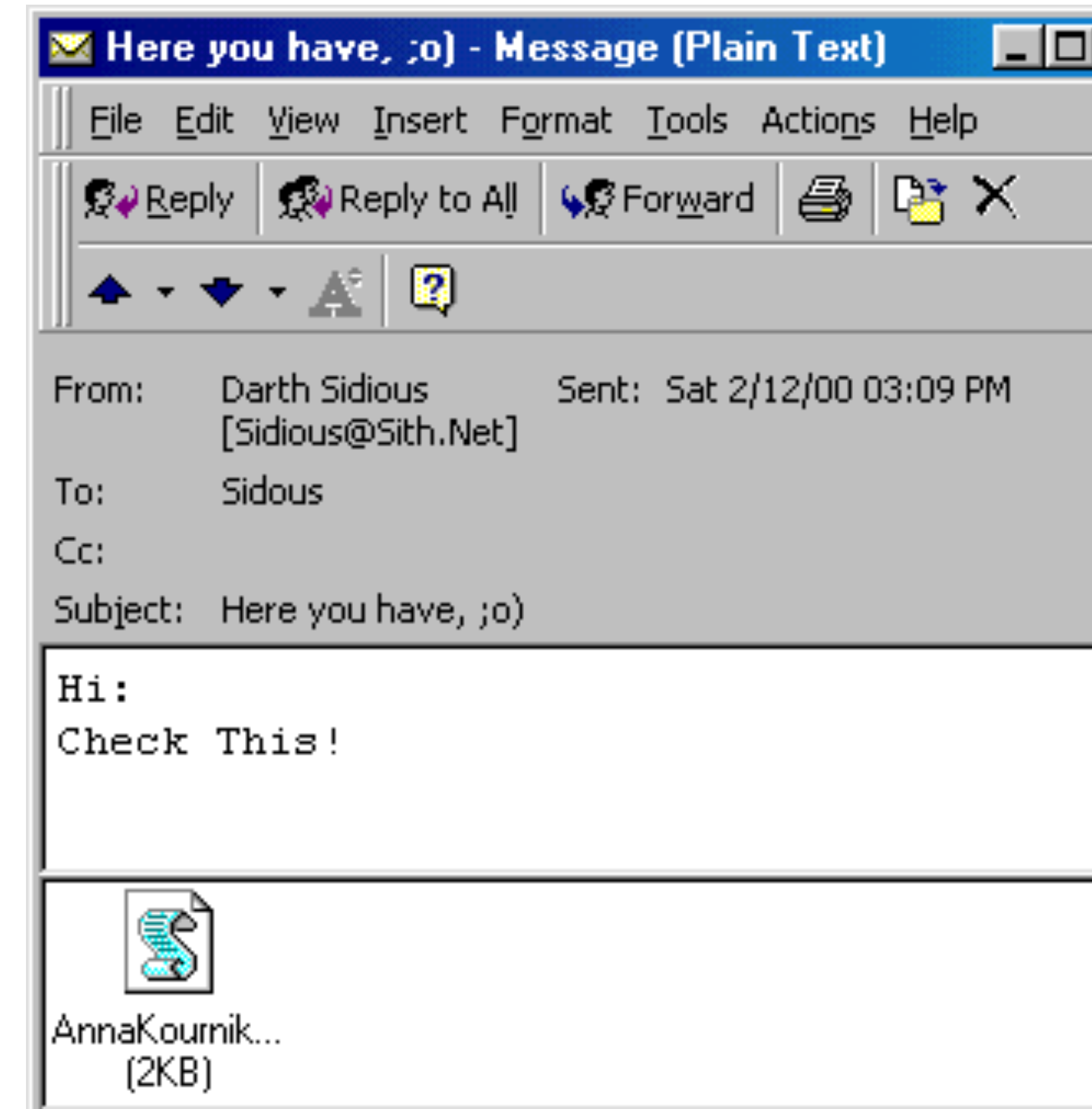
- Spread via emails on Feb 11<sup>th</sup>, 2001
- Attachment: AnnaKournikova.jpg.vbs



# Social Engineering 20yrs ago

## Anna Kournikova virus

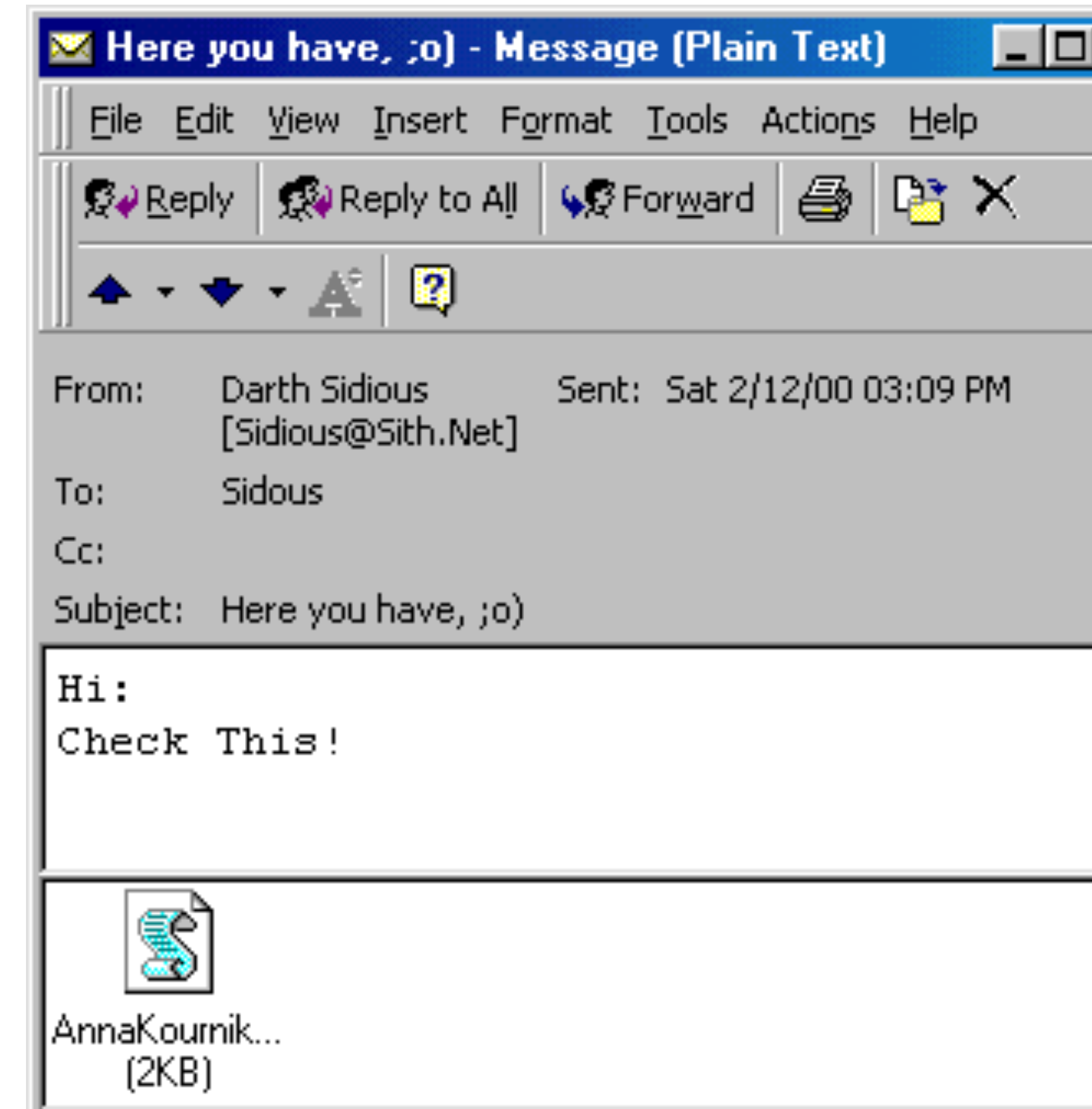
- Spread via emails on Feb 11<sup>th</sup>, 2001
- Attachment: AnnaKournikova.jpg.vbs
- Very simple virus, written in hours



# Social Engineering 20yrs ago

## Anna Kournikova virus

- Spread via emails on Feb 11<sup>th</sup>, 2001
- Attachment: AnnaKournikova.jpg.vbs
- Very simple virus, written in hours
- No local damage, but mail servers crashed



# Social Engineering Techniques



# Baiting



# Baiting

Very simple physical attack



# Baiting

Very simple physical attack

- 1) Preload USB keys with malware





# Baiting

Very simple physical attack

- 1) Preload USB keys with malware
- 2) Drop the keys in public, near victims



# Baiting

Very simple physical attack

- 1) Preload USB keys with malware
- 2) Drop the keys in public, near victims
- 3) Wait for victims to pick up and plug in



# Baiting

## Very simple physical attack

- 1) Preload USB keys with malware
- 2) Drop the keys in public, near victims
- 3) Wait for victims to pick up and plug in
- 4) Victim executes malware
  - Either by accident due to curiosity
  - Or autorun by the OS (e.g. Windows)



# Baiting



# Baiting

Does dropping USB drives really work?



# Baiting

Does dropping USB drives really work?

- Elie Bursztein, Black Hat 2016



# Baiting

Does dropping USB drives really work?

- Elie Bursztein, Black Hat 2016
- Dropped 297 USB sticks on the University of Illinois Urbana-Champaign campus



# Baiting

Does dropping USB drives really work?

- Elie Bursztein, Black Hat 2016
- Dropped 297 USB sticks on the University of Illinois Urbana-Champaign campus
- “Solutions to final exam”





# Baiting

Does dropping USB drives really work?

- Elie Bursztein, Black Hat 2016
- Dropped 297 USB sticks on the University of Illinois Urbana-Champaign campus
- “Solutions to final exam”
- 98% were picked up



# Baiting

Does dropping USB drives really work?

- Elie Bursztein, Black Hat 2016
- Dropped 297 USB sticks on the University of Illinois Urbana-Champaign campus
- “Solutions to final exam”
- 98% were picked up
- 45% were plugged in and someone clicked on files



# Baiting

Does dropping USB drives really work?

- Elie Bursztein, Black Hat 2016
- Dropped 297 USB sticks on the University of Illinois Urbana-Champaign campus
- “Solutions to final exam”
- 98% were picked up
- 45% were plugged in and someone clicked on files
- Black Hat presentation:

<https://www.youtube.com/watch?v=ZI5fvU5QKwQ>



# Baiting



# Baiting

- Stuxnet is a computer worm



# Baiting

- Stuxnet is a computer worm
- Targeted Iran's nuclear program



# Baiting

- Stuxnet is a computer worm
- Targeted Iran's nuclear program
- Discovered in 2010



# Baiting

- Stuxnet is a computer worm
- Targeted Iran's nuclear program
- Discovered in 2010
- Very sophisticated (exploit four zero-day flaws)





# Baiting

- Stuxnet is a computer worm
- Targeted Iran's nuclear program
- Discovered in 2010
- Very sophisticated (exploit four zero-day flaws)
- According to Snowden made by US and Israel



# Baiting

- Stuxnet is a computer worm
- Targeted Iran's nuclear program
- Discovered in 2010
- Very sophisticated (exploit four zero-day flaws)
- According to Snowden made by US and Israel
- Initially spread through infected USB flash drives



Quid Pro Quo

# Quid Pro Quo

- The attacker provides a service, whereas baiting usually takes the form of a good.



# Quid Pro Quo

- The attacker provides a service, whereas baiting usually takes the form of a good.
- Impersonate as a government entity and ask to confirm the SSN for the purpose of committing identity theft.



# Quid Pro Quo

- The attacker provides a service, whereas baiting usually takes the form of a good.
- Impersonate as a government entity and ask to confirm the SSN for the purpose of committing identity theft.
- People would give their password for chocolate



Quid pro quo

# Quid pro quo

- Edward Snowden is an ex-contractor for NSA





# Quid pro quo

- Edward Snowden is an ex-contractor for NSA
- Since 2013 he published thousands of super-secret classified NSA documents



# Quid pro quo

- Edward Snowden is an ex-contractor for NSA
- Since 2013 he published thousands of super-secret classified NSA documents



INTERNET NEWS NOVEMBER 7, 2013 / 10:07 PM / UPDATED 7 YEARS AGO

## Exclusive: Snowden persuaded other NSA workers to give up passwords - sources

By Mark Hosenball, Warren Strobel

4 MIN READ

# Quid pro quo

- Edward Snowden is an ex-contractor for NSA
- Since 2013 he published thousands of super-secret classified NSA documents
- When stationed in a spy base in Hawaii, 20-25 NSA employees gave their passwords to Snowden



INTERNET NEWS NOVEMBER 7, 2013 / 10:07 PM / UPDATED 7 YEARS AGO

**Exclusive: Snowden persuaded other NSA workers to give up passwords - sources**

By Mark Hosenball, Warren Strobel

4 MIN READ

# Quid pro quo

- Edward Snowden is an ex-contractor for NSA
- Since 2013 he published thousands of super-secret classified NSA documents
- When stationed in a spy base in Hawaii, 20-25 NSA employees gave their passwords to Snowden
- Snowden convinced them he needed the login details to do his job as a systems admin



INTERNET NEWS NOVEMBER 7, 2013 / 10:07 PM / UPDATED 7 YEARS AGO

**Exclusive: Snowden persuaded other NSA workers to give up passwords - sources**

By Mark Hosenball, Warren Strobel

4 MIN READ

# Dumpster diving

# Dumpster diving

Going through trashcans and dumpsters looking for information



# Dumpster diving

Going through trashcans and dumpsters looking for information

- IP addresses, usernames, passwords, emails



# Dumpster diving

Going through trashcans and dumpsters looking for information

- IP addresses, usernames, passwords, emails
- Medical records, resumes, bank statements





# Dumpster diving

Going through trashcans and dumpsters looking for information

- IP addresses, usernames, passwords, emails
- Medical records, resumes, bank statements
- Old computers



# Dumpster diving

Going through trashcans and dumpsters looking for information

- IP addresses, usernames, passwords, emails
- Medical records, resumes, bank statements
- Old computers



[www.thebalancesmb.com](http://www.thebalancesmb.com)



<http://www.subliminalhacking.net/>



Pittsburgh's Action News 4, 2017

# Tailgating



# Tailgating

Enable an attacker entering a restricted area



# Tailgating

Enable an attacker entering a restricted area

- Walk behind an authorized person



<https://trustaira.com/>



<https://en.wikipedia.org/>

# Tailgating

Enable an attacker entering a restricted area

- Walk behind an authorized person
- Impersonate delivery man holding package asking to hold the door



<https://trustaira.com/>



<https://en.wikipedia.org/>

# Tailgating

Enable an attacker entering a restricted area

- Walk behind an authorized person
- Impersonate delivery man holding package asking to hold the door
- Join smokers next to a side door



<https://trustaira.com/>



<https://en.wikipedia.org/>



# Tailgating

Enable an attacker entering a restricted area

- Walk behind an authorized person
- Impersonate delivery man holding package asking to hold the door
- Join smokers next to a side door

Once in the building can access to internal networks, workstations, etc.



<https://trustaira.com/>



<https://en.wikipedia.org/>

# Tailgating

Enable an attacker entering a restricted area

- Walk behind an authorized person
- Impersonate delivery man holding package asking to hold the door
- Join smokers next to a side door

Once in the building can access to internal networks, workstations, etc.



<https://trustaira.com/>



<https://en.wikipedia.org/>

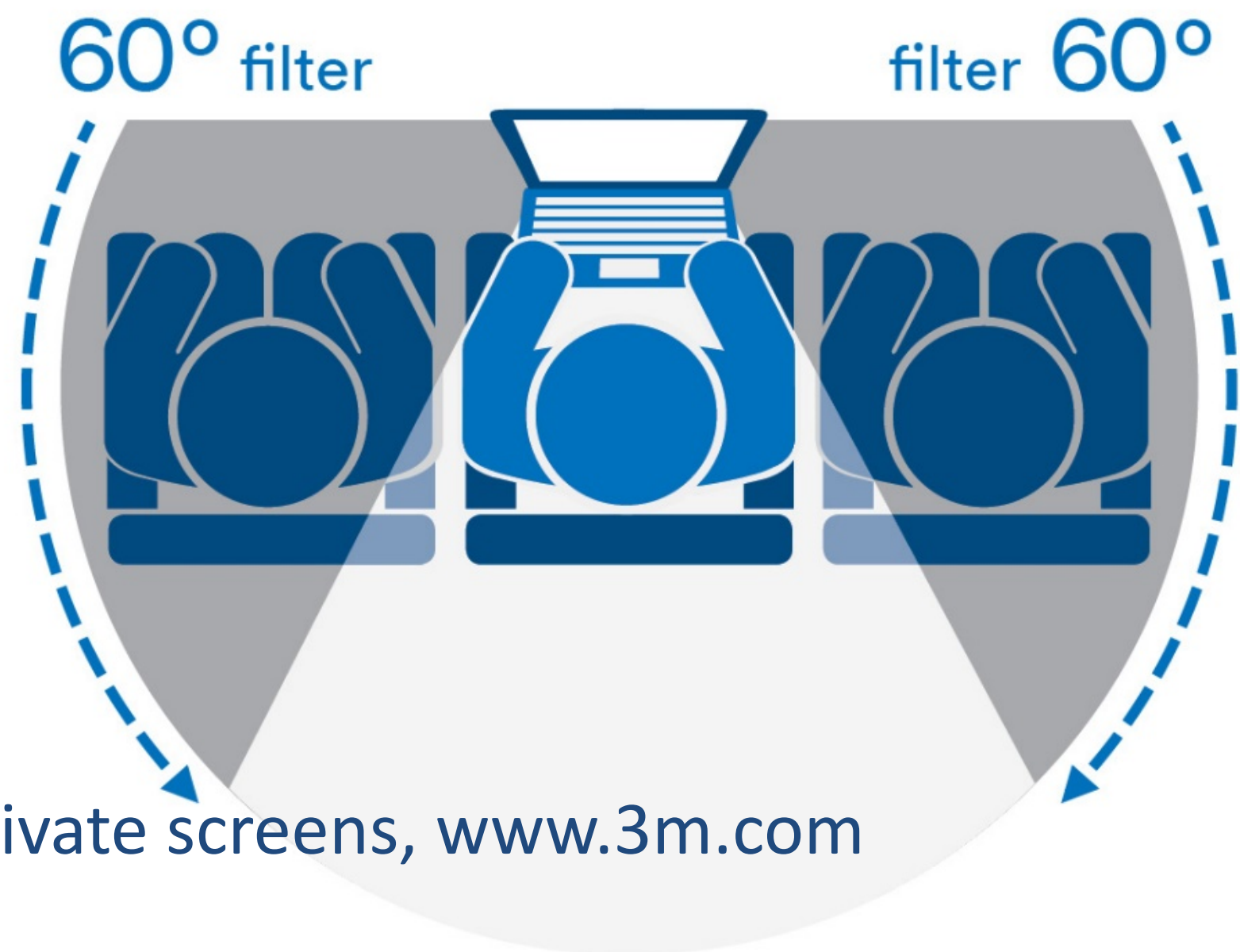
Shoulder surfing

# Shoulder surfing



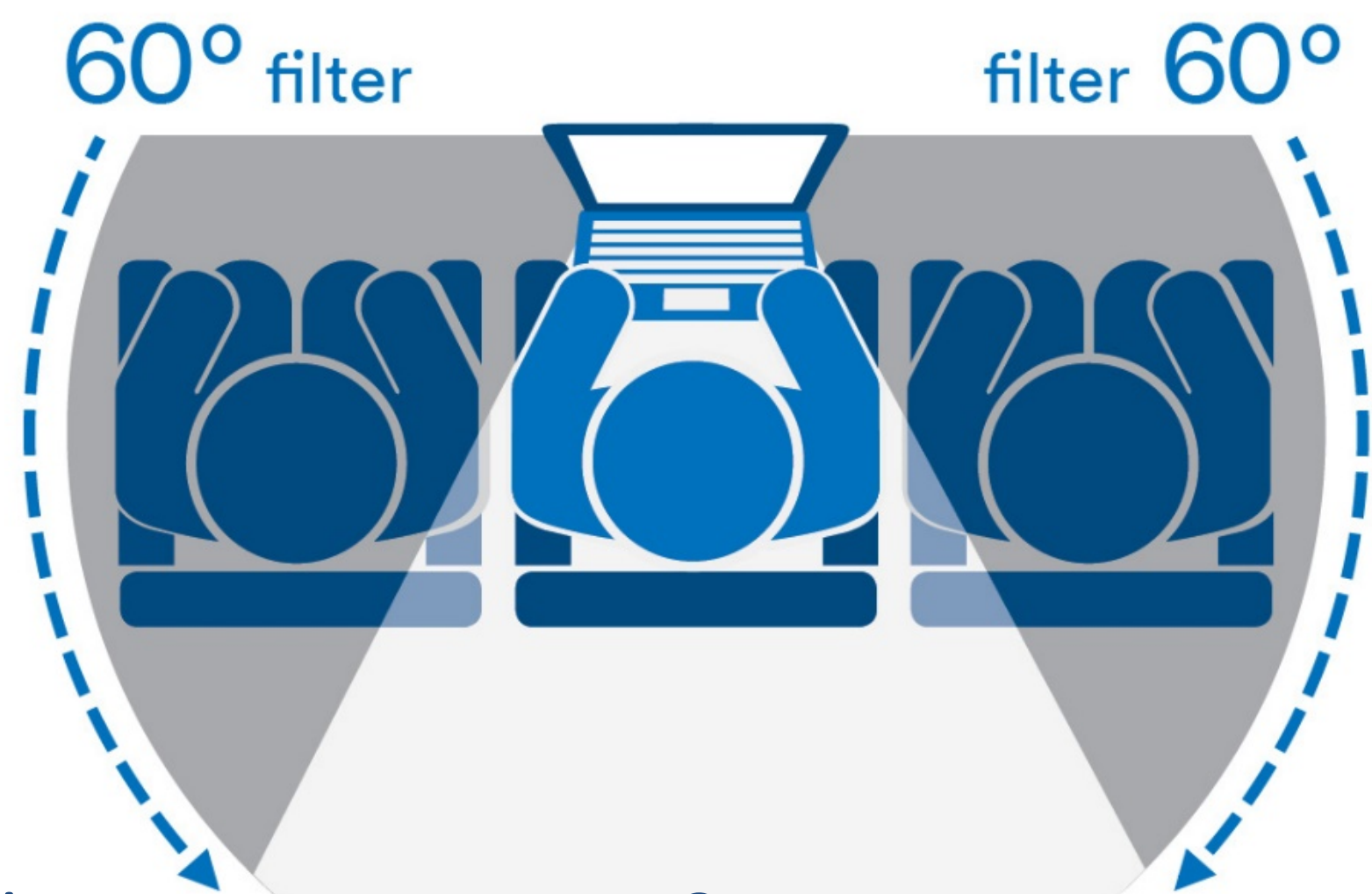
<https://travelskills.com/>

# Shoulder surfing



<https://travelskills.com/>

# Shoulder surfing



Private screens, [www.3m.com](http://www.3m.com)



<https://travelskills.com/>

# Pre-texting



# Pre-texting

- Manipulate victims into divulging sensitive information





# Pre-texting

- Manipulate victims into divulging sensitive information
- Creating false trust



# Pre-texting

- Manipulate victims into divulging sensitive information
- Creating false trust
- Email from head of IT support



# Pre-texting

- Manipulate victims into divulging sensitive information
- Creating false trust
- Email from head of IT support
- Illustration:  
<https://www.youtube.com/watch?v=BllvsJ3yi8o>



# Phishing



[www.123rf.com](http://www.123rf.com)

# Phishing

- Attempt to steal users' sensitive data



[www.123rf.com](http://www.123rf.com)

# Phishing

- Attempt to steal users' sensitive data
- E.g., login credentials, credit card numbers, SSN, bank accounts, etc.



[www.123rf.com](http://www.123rf.com)

# Phishing

- Attempt to steal users' sensitive data
- E.g., login credentials, credit card numbers, SSN, bank accounts, etc.
- Spreads via emails, SMS, IM, social media



[www.123rf.com](http://www.123rf.com)

# Phishing

- Attempt to steal users' sensitive data
- E.g., login credentials, credit card numbers, SSN, bank accounts, etc.
- Spreads via emails, SMS, IM, social media
- The recipient is tricked into clicking a malicious link:
  - Install malware
  - Redirect to malicious website



[www.123rf.com](http://www.123rf.com)



# Phishing

# Phishing

- Most common form of social engineering cyber attack

# Phishing

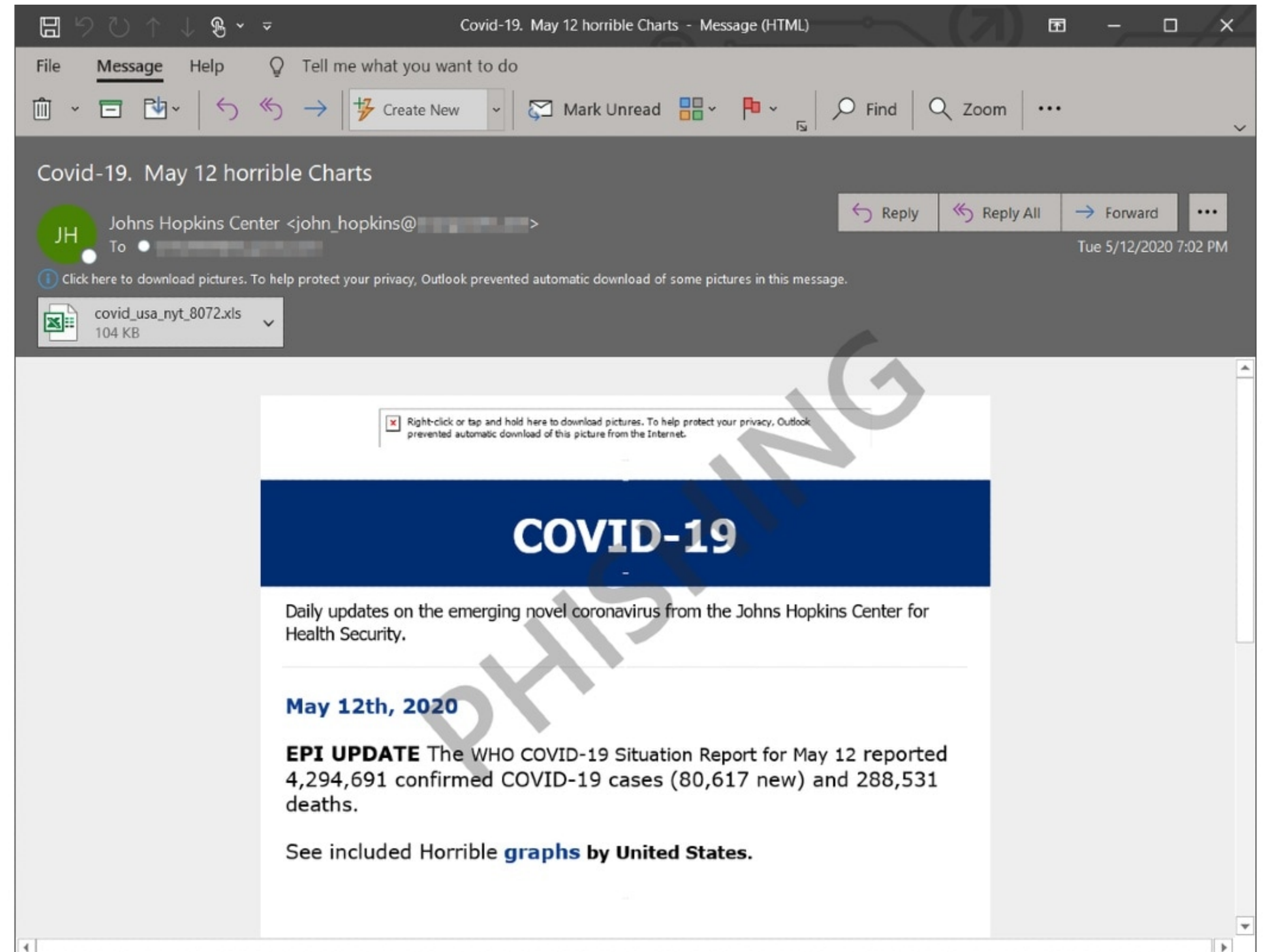
- Most common form of social engineering cyber attack
- In 2014:
  - 90% of all emails are spam
  - 77% of SE-based attacks rely on phishing
  - 88% of recorded phishing involve clicking links in emails

# Phishing

- Most common form of social engineering cyber attack
- In 2014:
  - 90% of all emails are spam
  - 77% of SE-based attacks rely on phishing
  - 88% of recorded phishing involve clicking links in emails

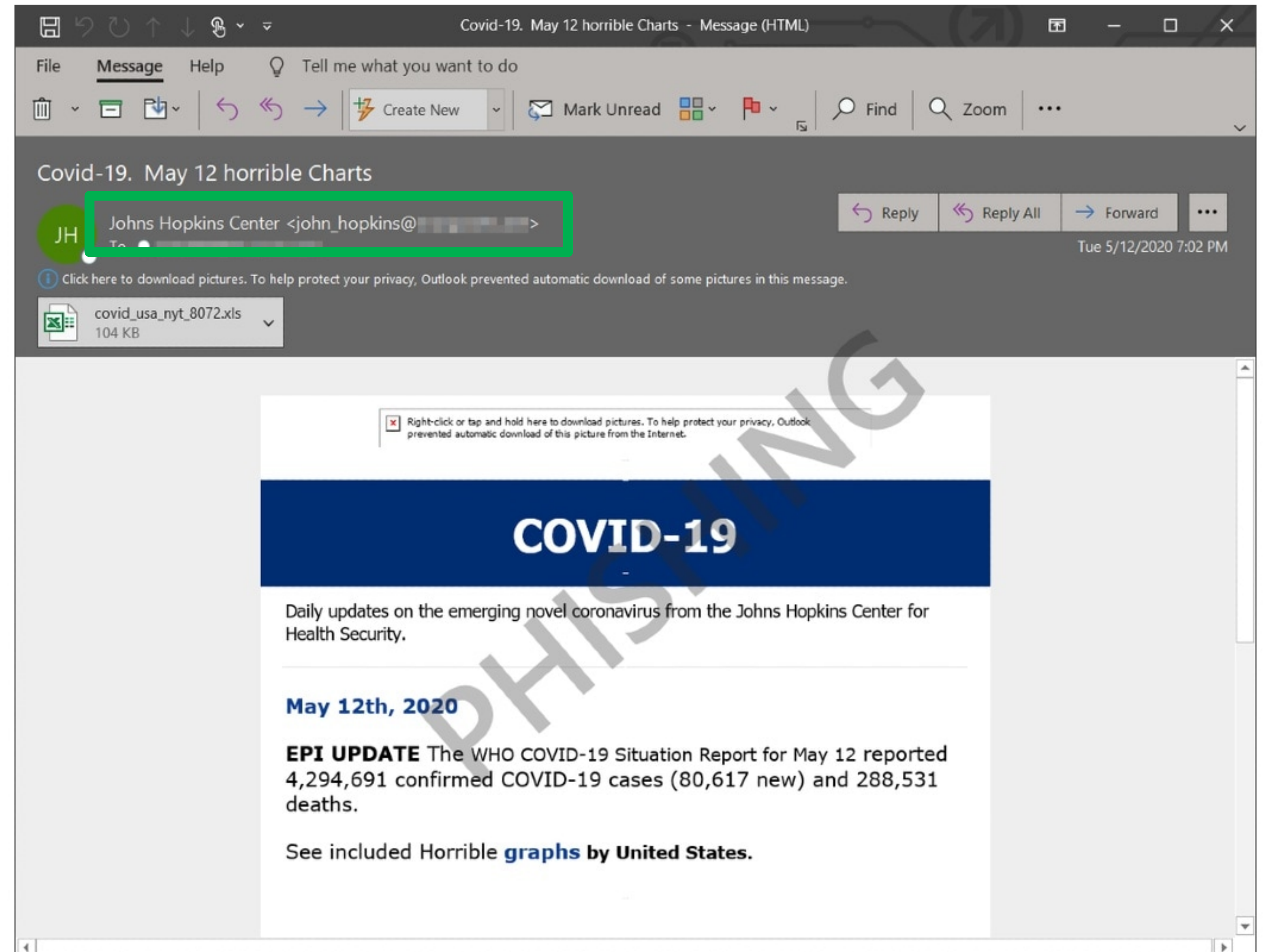
# Phishing

- In April/May 2020, Microsoft discovered a phishing campaign based on COVID-19
- Opening the Excel file opens a pop-up to enable macros
- Accepting installs a RAT (Remote Access Trojan)



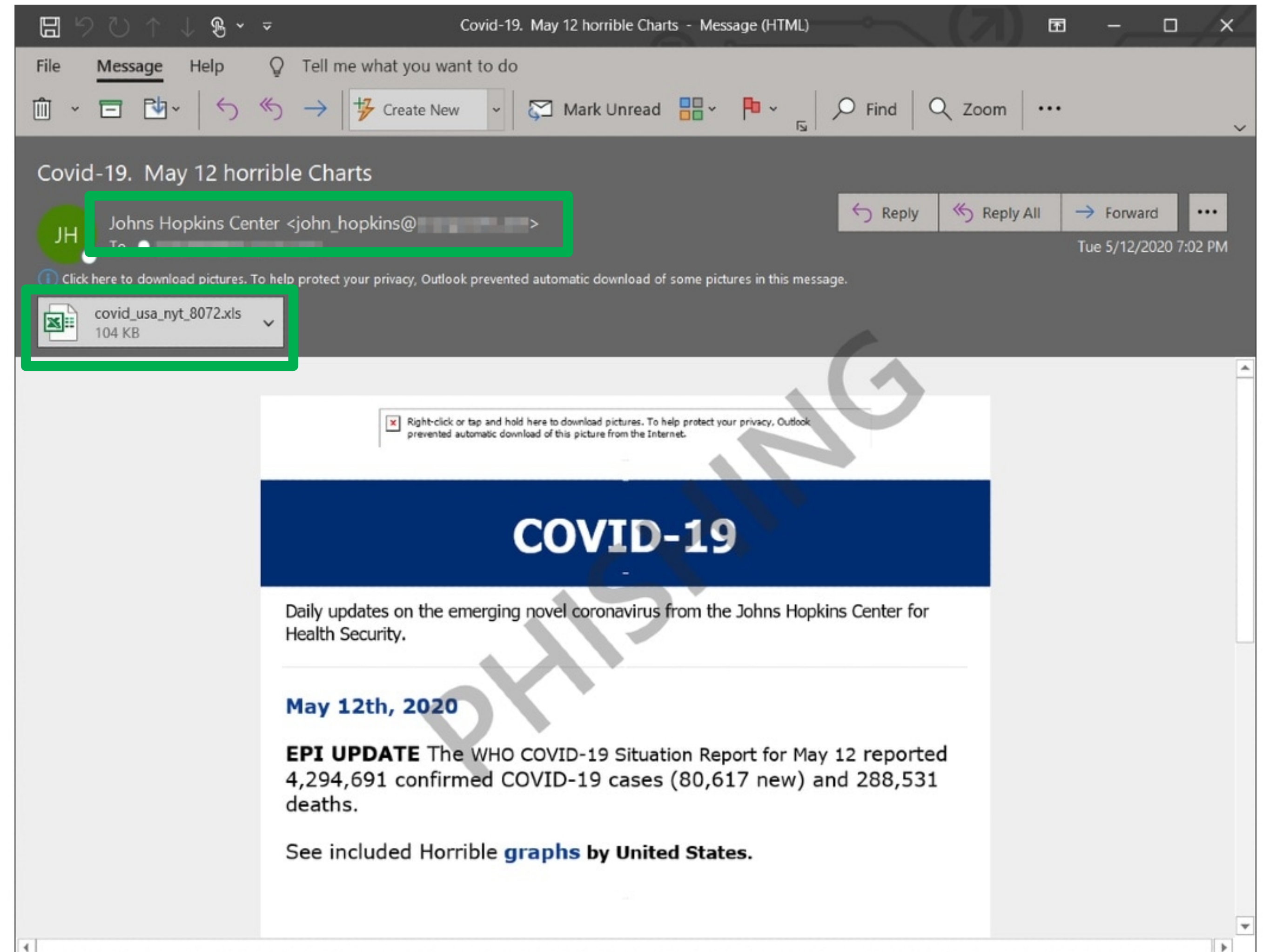
# Phishing

- In April/May 2020, Microsoft discovered a phishing campaign based on COVID-19
- Opening the Excel file opens a pop-up to enable macros
- Accepting installs a RAT (Remote Access Trojan)

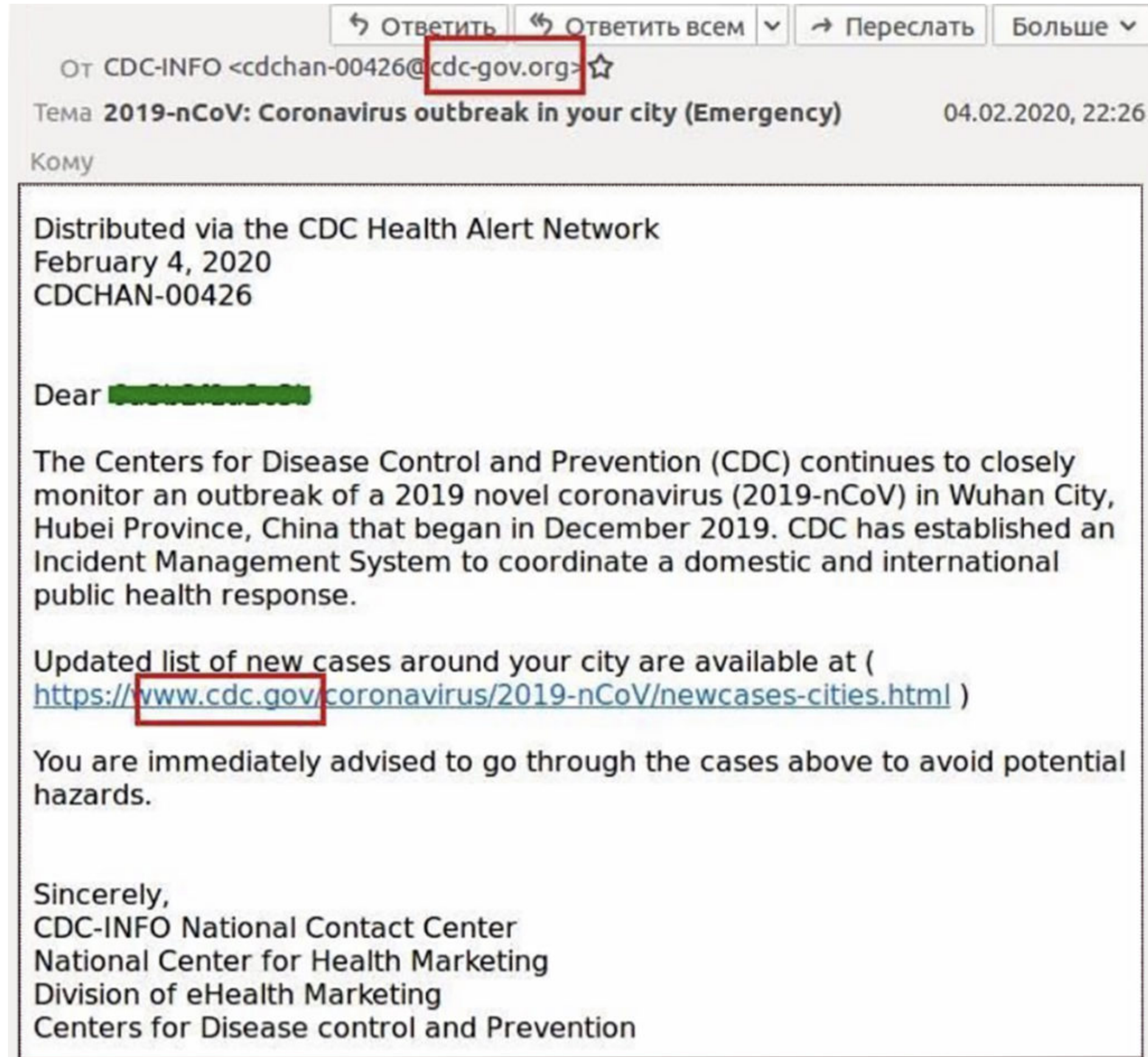


# Phishing

- In April/May 2020, Microsoft discovered a phishing campaign based on COVID-19
- Opening the Excel file opens a pop-up to enable macros
- Accepting installs a RAT (Remote Access Trojan)

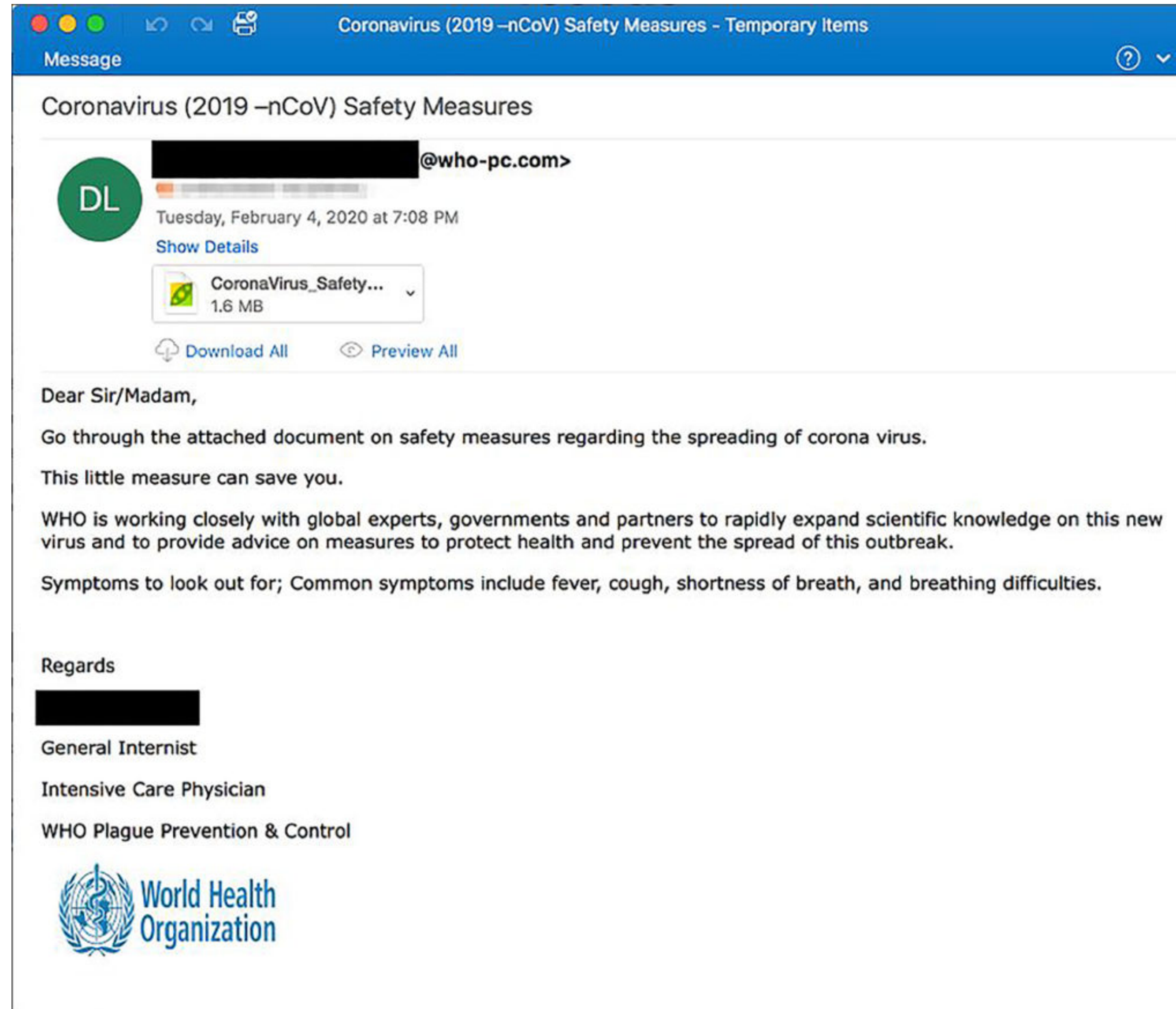


# Phishing






# Phishing




# Phishing

The image shows a screenshot of a web browser displaying a phishing website that mimics the Bank of the West homepage. The browser's address bar shows the URL `http://www.bankofthewest.com/BOW/home/index.html`. The page layout includes a navigation menu with links for [PERSONAL](#), [SMALL BUSINESS](#), [COMMERCIAL](#), and [ABOUT US](#). A large banner features a bear swimming in water with the text **HOME EQUITY** and the subtext "Get in on the Great Rate Lock-in! Click here for the key". On the left side, there is a "Sign In" section for "eTimeBanker®" with fields for "User Name:" and "Password:", a "SIGN IN" button, and a "Forgot Password?" link. Below this is a section for "Other Online Services" with a dropdown menu and a "GO" button. Further down is a "Locations" section with a "State:" dropdown (set to "All") and a "ZIP code:" field, accompanied by a "LOCATE" button. At the bottom left, a "CONSUMER ALERT!" box contains the text "Tips on protecting yourself and". On the right side, there are sections for "Personal Banking" and "Small Business Banking". The "Personal Banking" section includes a welcome message and a list of services: [Checking](#), [Savings & CDs](#), [Debit & Credit Cards](#), [Online Banking](#), [Wealth & Trust](#), [Consumer Loans](#), [Private Banking](#), and [More ...](#). The "Small Business Banking" section includes a tagline "Taking care of business. Across town. Around the globe.", a paragraph of text, and links for [Business Checking](#) and [Loans & Lines](#).

Friday, July 29, 2005      中文 Chinese | [Locations](#) | [Employment](#) | [Contact Us](#) | Search:

**BANK OF THE WEST**       [PERSONAL](#)   [SMALL BUSINESS](#)   [COMMERCIAL](#)   [ABOUT US](#)

**Online Banking**  
[Learn More](#) | [Enroll Online](#)  
eTimeBanker® Sign In:  
User Name:   
Password:    
[Forgot Password?](#)   
Other Online Services:

**Locations**  
State:    
ZIP code:

**CONSUMER ALERT!**  
Tips on protecting yourself and


**HOME EQUITY**  
Get in on the Great Rate Lock-in! [Click here for the key](#)

**Personal Banking**  
Welcome to your community bank.  
First job. Last job. New home. College tuition. We're here to help guide your finances through the challenges of every life stage. Stop by a branch to experience our hallmark service for yourself.  
[Checking](#)      [Wealth & Trust](#)  
[Savings & CDs](#)      [Consumer Loans](#)  
[Debit & Credit Cards](#)      [Private Banking](#)  
[Online Banking](#)      [More ...](#)

**Small Business Banking**  
Taking care of business. Across town. Around the globe.  
As you navigate your business through all its cycles, you're not on your own. We assign a dedicated relationship manager to help you make the right financial choices. Give us a call. We pick up the phone!  
[Business Checking](#)      [Loans & Lines](#)

# Phishing


Friday, July 29, 2005      中文 Chinese | Locations | Employment | Contact Us | Search:

**BANK OF THE WEST**       [PERSONAL](#)   [SMALL BUSINESS](#)   [COMMERCIAL](#)   [ABOUT US](#)


### Online Banking

[Learn More](#) | [Enroll Online](#)  
eTimeBanker® Sign In:


User Name:   
Password:

[Forgot Password?](#) 

Other Online Services:



## HOME EQUITY

Get in on the Great Rate Lock-in! [Click here for the key](#) 

### Personal Banking

**Welcome to your community bank.**  
First job. Last job. New home. College tuition. We're here to help guide your finances through the challenges of every life stage. Stop by a branch to experience our hallmark service for yourself.

[Checking](#)      [Wealth & Trust](#)  
[Savings & CDs](#)      [Consumer Loans](#)  
[Debit & Credit Cards](#)      [Private Banking](#)  
[Online Banking](#)      [More ...](#)

### Small Business Banking

**Taking care of business. Across town. Around the globe.**  
As you navigate your business through all its cycles, you're not on your own. We assign a dedicated relationship manager to help you make the right financial choices. Give us a call. We pick up the phone!

[Business Checking](#)      [Loans & Lines](#)

**CONSUMER ALERT!**  
Tips on protecting yourself and

# Phishing

<https://www.phishingbox.com/phishing-test>



# Vishing

# Vishing

- Phone-based phishing

# Vishing

- Phone-based phishing
- Using caller-id spoofing

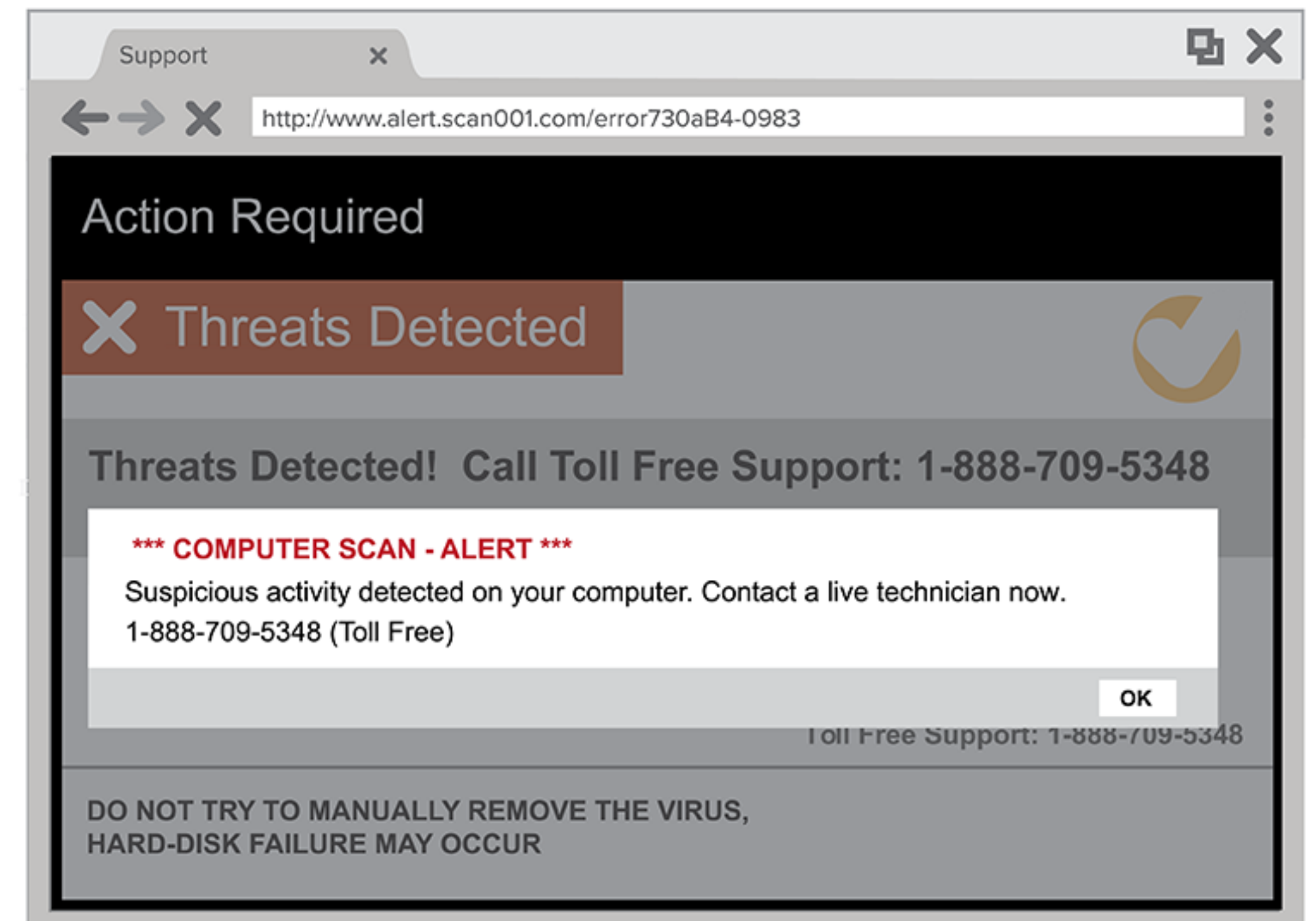
# Vishing

- Phone-based phishing
- Using caller-id spoofing
- Get the target to call a bogus 1-800 number



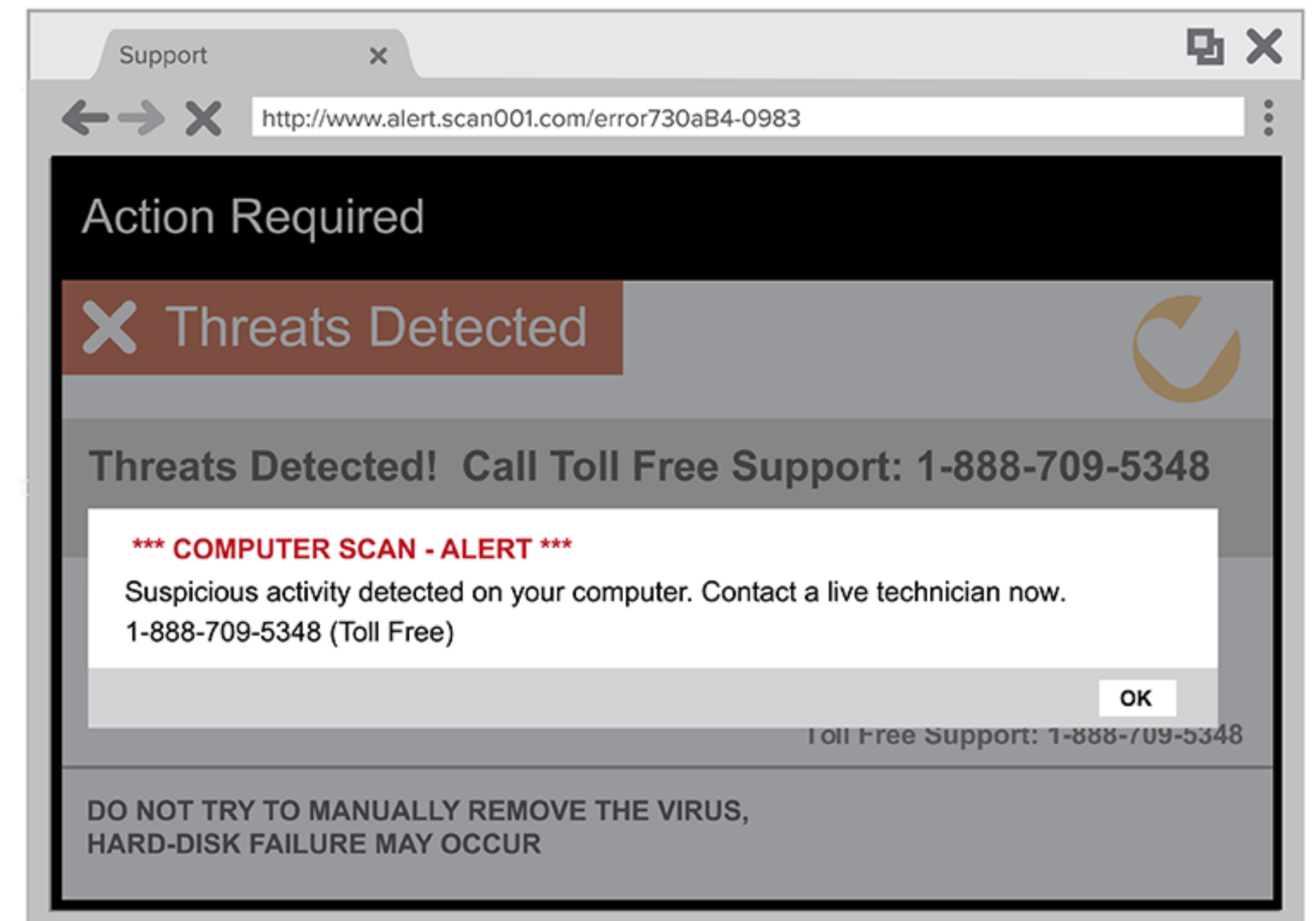
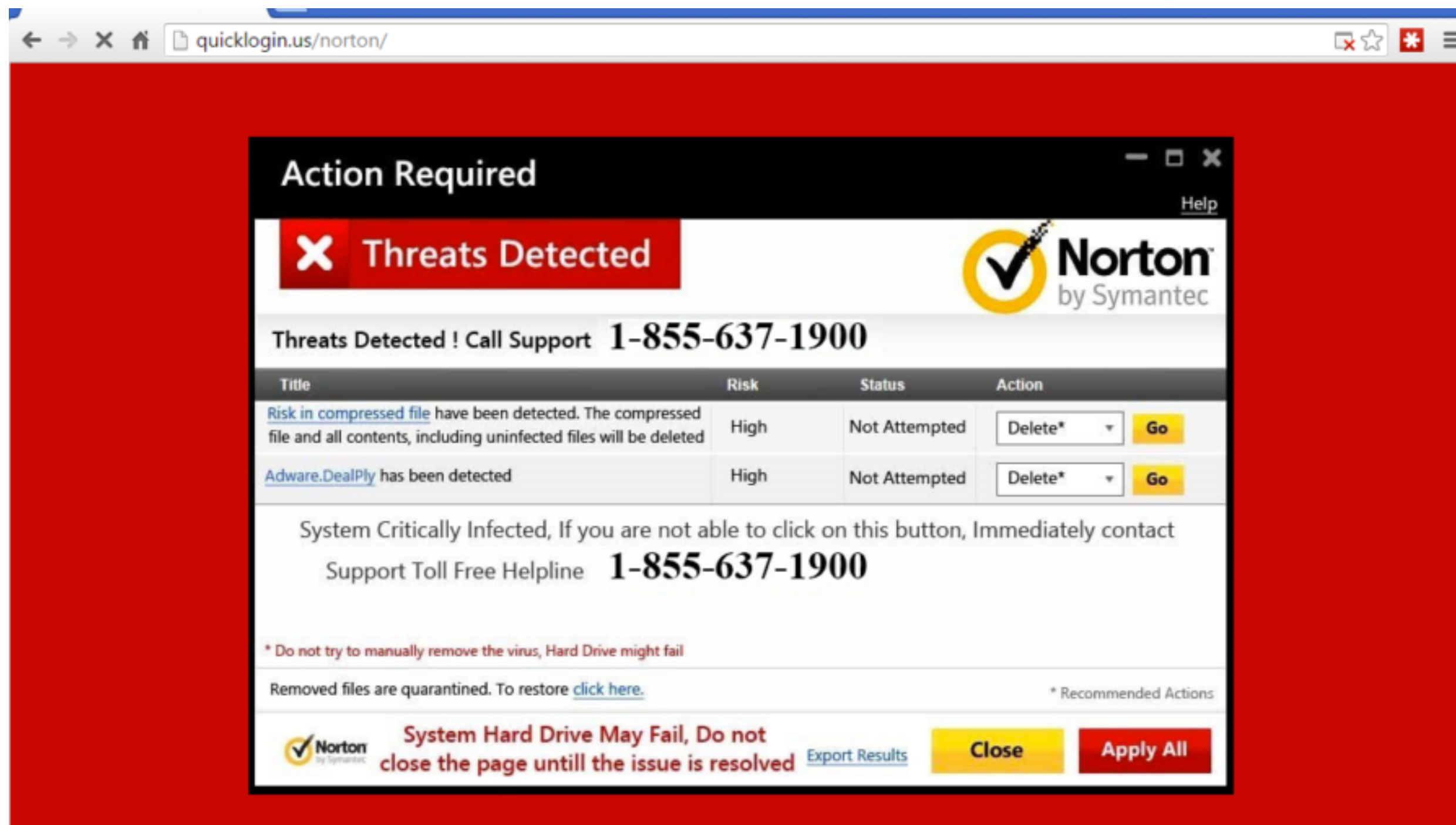
# Vishing

- Phone-based phishing
- Using caller-id spoofing
- Get the target to call a bogus 1-800 number



# Vishing

- Phone-based phishing
- Using caller-id spoofing
- Get the target to call a bogus 1-800 number



# SMiShing

# SMiShing



# SMiShing



Text Message  
Today 9:45 AM

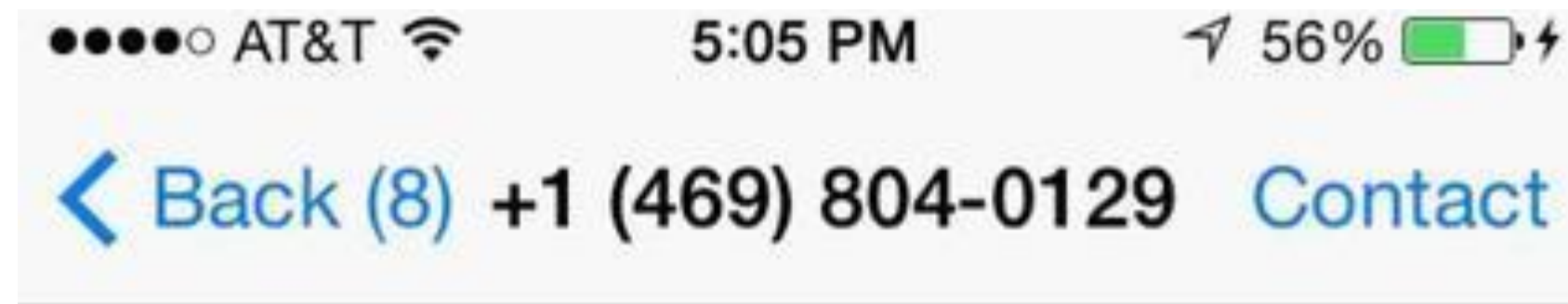
Debit-card SUSPENDED !  
Click to reactivate: <http://themis.pe/service.clearview-federal-credit-union.html>



Text Message  
Today 01:15

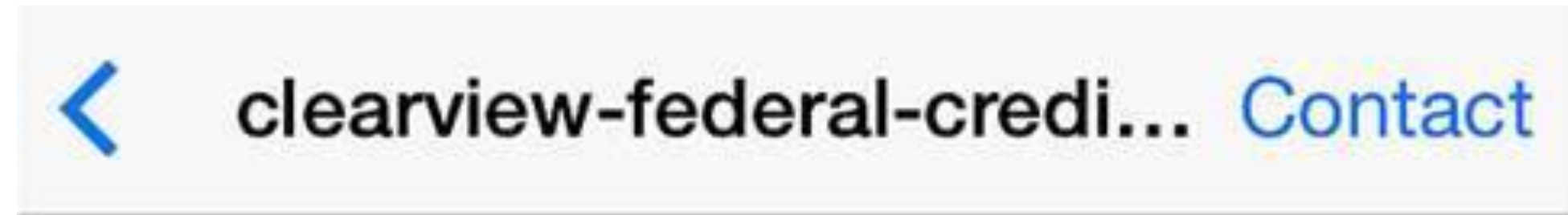
Dear Customer,  
  
Your AppleID is due to expire Today, Please tap <http://bit.do/cRqb6> to update and prevent loss of services and data.  
  
Apple smsSTOPto43420

# SMiShing



Text Message  
Today 5:04 PM

wtf, why did you post my pic on fb?? <https://bitly.com/1Ac3yQN>



Text Message  
Today 9:45 AM

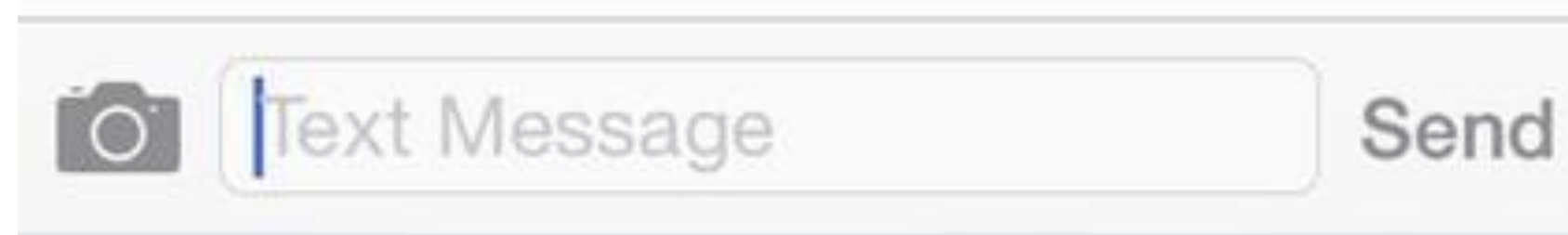
Debit-card SUSPENDED !  
Click to reactivate: <http://themis.pe/service.clearview-federal-credit-union.html>



Text Message  
Today 01:15

Dear Customer,  
  
Your AppleID is due to expire Today, Please tap <http://bit.do/cRqb6> to update and prevent loss of services and data.

Apple smsSTOPto43420



# Water-hole attack



# Water-hole attack

- “Phishing without a lure”





# Water-hole attack

- “Phishing without a lure”
- Monitor which websites the targets browse



# Water-hole attack

- “Phishing without a lure”
- Monitor which websites the targets browse
- If those websites are vulnerable infect them



# Water-hole attack

- “Phishing without a lure”
- Monitor which websites the targets browse
- If those websites are vulnerable infect them
- 2012 US Council on Foreign Relations was infected with 0-day vulnerability in Internet Explorer  
Triggered when language was set to English, Chinese, Japanese, Korean and Russian

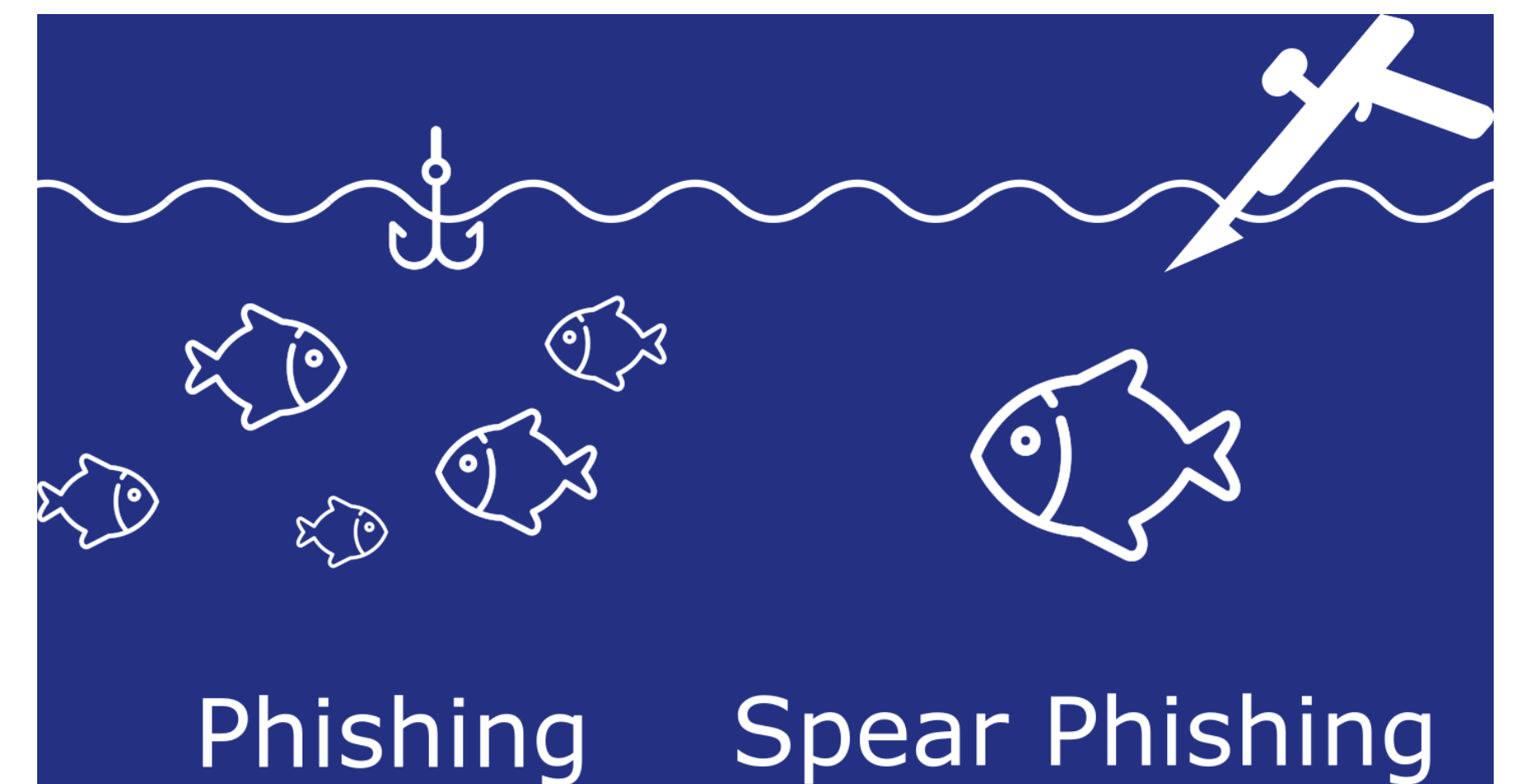


# Water-hole attack

- “Phishing without a lure”
- Monitor which websites the targets browse
- If those websites are vulnerable infect them
- 2012 US Council on Foreign Relations was infected with 0-day vulnerability in Internet Explorer  
Triggered when language was set to English, Chinese, Japanese, Korean and Russian
- 2015 attack on Forbes.com showed malicious versions of ‘Thought of the Day’ leveraging 2 zero-day vulnerabilities (Internet Explorer & Flash)

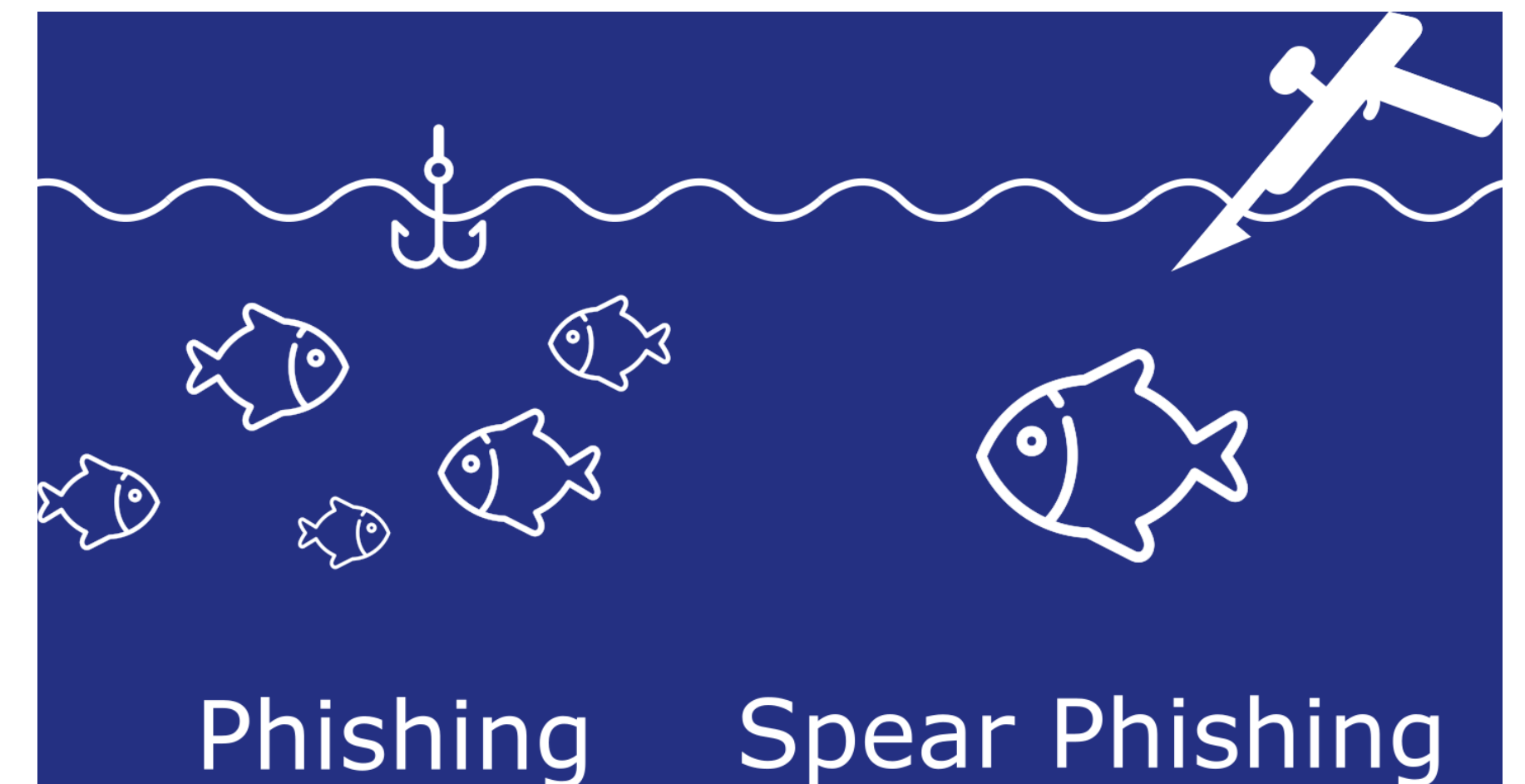


# Spear Phishing



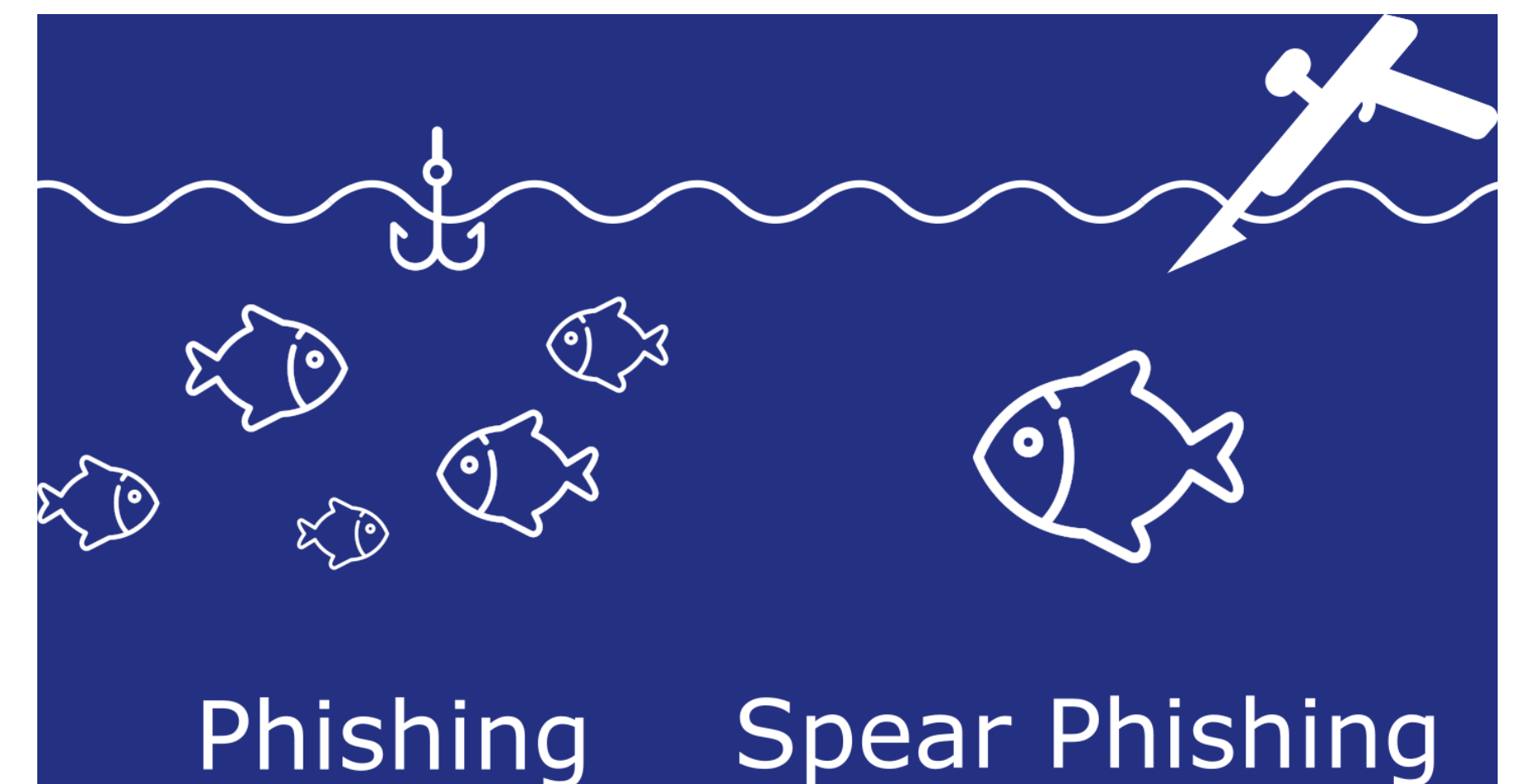
# Spear Phishing

- Highly targeted phishing attack



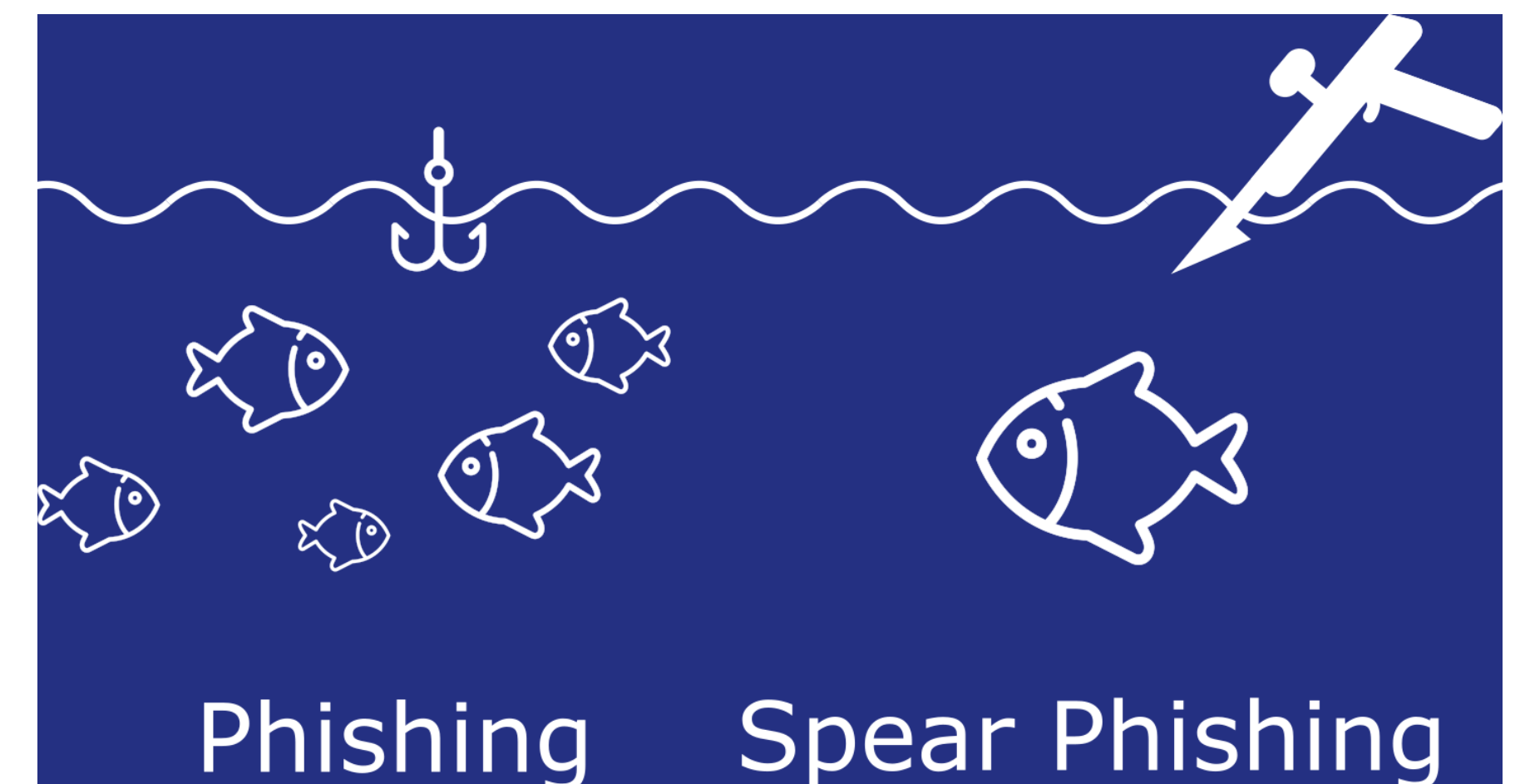
# Spear Phishing

- Highly targeted phishing attack
- Involves a lot of background research: social media, corporate websites, publicly available information



# Spear Phishing

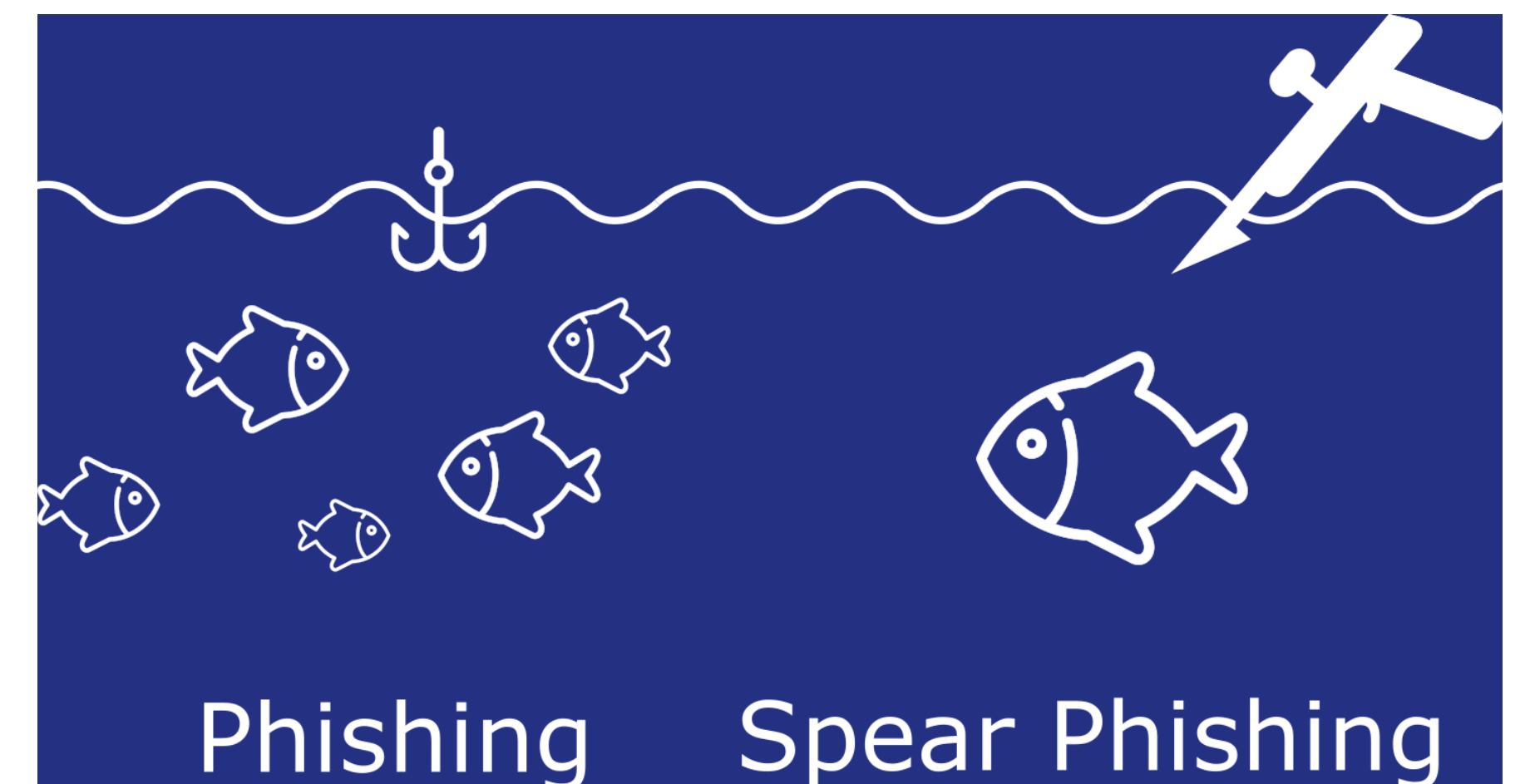
- Highly targeted phishing attack
- Involves a lot of background research: social media, corporate websites, publicly available information
- Does not trigger spam filters





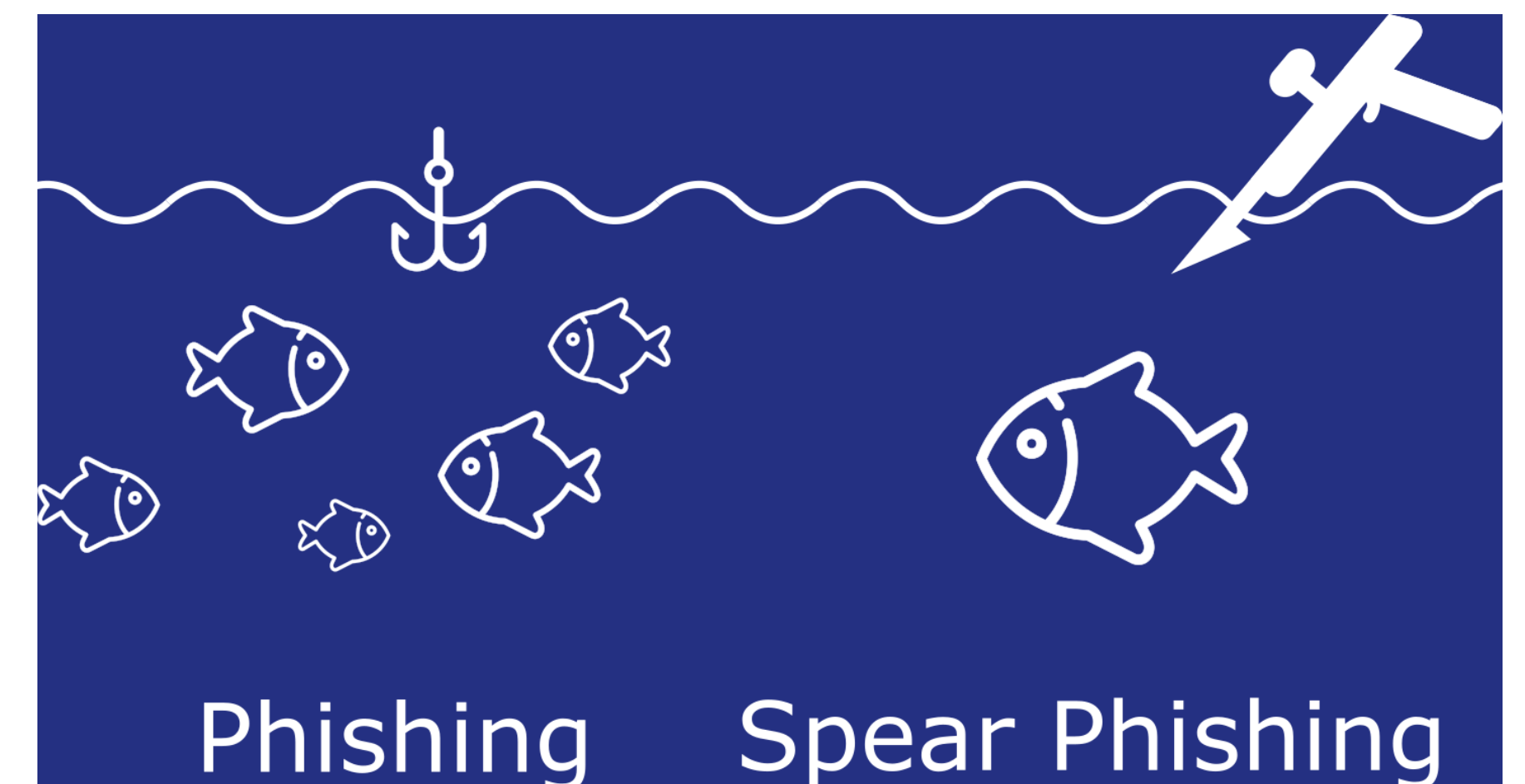
# Spear Phishing

- Highly targeted phishing attack
- Involves a lot of background research: social media, corporate websites, publicly available information
- Does not trigger spam filters
- Very challenging to detect by people and anomaly detectors



# Spear Phishing

- Highly targeted phishing attack
- Involves a lot of background research: social media, corporate websites, publicly available information
- Does not trigger spam filters
- Very challenging to detect by people and anomaly detectors
- May be sent from hacked, legit email accounts



# John Podesta Phishing Email

# John Podesta Phishing Email

- Campaign manager of Hillary Clinton

# John Podesta Phishing Email

- Campaign manager of Hillary Clinton
- On March 19, 2016 received a Google security alert

# John Podesta Phishing Email

- Campaign manager of Hillary Clinton
- On March 19, 2016 received a Google security alert



## Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account  
[john.podesta@gmail.com](mailto:john.podesta@gmail.com).

### Details:

Saturday, 19 March, 8:34:30 UTC

IP Address: 134.249.139.239

Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

**CHANGE PASSWORD**

Best,  
The Gmail Team

# John Podesta Phishing Email

- Campaign manager of Hillary Clinton
- On March 19, 2016 received a Google security alert
- This was a spear-fishing attack by Russian intelligence

Google



## Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account  
[john.podesta@gmail.com](mailto:john.podesta@gmail.com).

### Details:

Saturday, 19 March, 8:34:30 UTC  
IP Address: 134.249.139.239  
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

[CHANGE PASSWORD](#)

Best,  
The Gmail Team

# John Podesta Phishing Email

```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [REDACTED]@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [REDACTED]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```

[www.cbsnews.com](http://www.cbsnews.com)



# John Podesta Phishing Email

- Campaign manager of Hillary Clinton

```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [REDACTED]@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [REDACTED]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```

[www.cbsnews.com](http://www.cbsnews.com)

# John Podesta Phishing Email

- Campaign manager of Hillary Clinton
- On March 19, 2016 received a Google security alert

```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [REDACTED]@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [REDACTED]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```

# John Podesta Phishing Email

- Campaign manager of Hillary Clinton
- On March 19, 2016 received a Google security alert
- This was a spear-fishing attack by Russian intelligence
- Podesta forward the email to his chief of staff, Sara Latham, who asked IT support

\*Subject:\* \*Re: Someone has your password\*

Sara,

This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

He can go to this link: <https://myaccount.google.com/security> to do both. It is absolutely imperative that this is done ASAP.

If you or he has any questions, please reach out to me at 410.562.9762

```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [REDACTED]@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [REDACTED]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```

[www.cbsnews.com](http://www.cbsnews.com)

# John Podesta Phishing Email

```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [REDACTED]@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [REDACTED]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```

[www.cbsnews.com](http://www.cbsnews.com)

# John Podesta Phishing Email

- Campaign manager of Hillary Clinton

```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [REDACTED]@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [REDACTED]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```

[www.cbsnews.com](http://www.cbsnews.com)

# John Podesta Phishing Email

- Campaign manager of Hillary Clinton
- On March 19, 2016 received a Google security alert

```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [REDACTED]@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [REDACTED]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```

# John Podesta Phishing Email

- Campaign manager of Hillary Clinton
- On March 19, 2016 received a Google security alert
- This was a spear-fishing attack by Russian intelligence
- Podesta forward the email to his chief of staff, Sara Latham, who asked IT support
- IT erroneously responded 'this is a legitimate email'
- Account compromised, emails dumped to Wikileaks
- Massive political scandal

```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [REDACTED]@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [REDACTED]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```

# John Podesta Phishing Email

- Campaign manager of Hillary Clinton
- On March 19, 2016 received a Google security alert
- This was a spear-fishing attack by Russian intelligence
- Podesta forward the email to his chief of staff, Sara Latham, who asked IT support
- IT erroneously responded 'this is a legitimate email'
- Account compromised, emails dumped to Wikileaks
- Massive political scandal

```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [REDACTED]@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [REDACTED]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```



# John Podesta Phishing Email

- Campaign manager of Hillary Clinton
- On March 19, 2016 received a Google security alert
- This was a spear-fishing attack by Russian intelligence
- Podesta forward the email to his chief of staff, Sara Latham, who asked IT support
- IT erroneously responded 'this is a legitimate email'
- Account compromised, emails dumped to Wikileaks
- Massive political scandal

```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [REDACTED]@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [REDACTED]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```

# John Podesta Phishing Email

- Campaign manager of Hillary Clinton
- On March 19, 2016 received a Google security alert
- This was a spear-fishing attack by Russian intelligence
- Podesta forward the email to his chief of staff, Sara Latham, who asked IT support
- IT erroneously responded 'this is a legitimate email'
- Account compromised, emails dumped to Wikileaks
- Massive political scandal

```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [REDACTED]@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [REDACTED]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```

# John Podesta Phishing Email

- Campaign manager of Hillary Clinton
- On March 19, 2016 received a Google security alert
- This was a spear-fishing attack by Russian intelligence
- Podesta forward the email to his chief of staff, Sara Latham, who asked IT support
- IT erroneously responded 'this is a legitimate email'
- Account compromised, emails dumped to Wikileaks
- Massive political scandal

```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [REDACTED]@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [REDACTED]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```

# John Podesta Phishing Email

- Bitly is a URL shortening service
- Bitly link is <https://bit.ly/1PibSU0>
- Expands to [http:// myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Ric3RhQGdtYWlsLmNvbQ==&fn=Sm9obiBQb2Ric3Rh&n=Sm9obg== ...](http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Ric3RhQGdtYWlsLmNvbQ==&fn=Sm9obiBQb2Ric3Rh&n=Sm9obg==)
- The top-level domain is **com-securitysettingpage.tk**

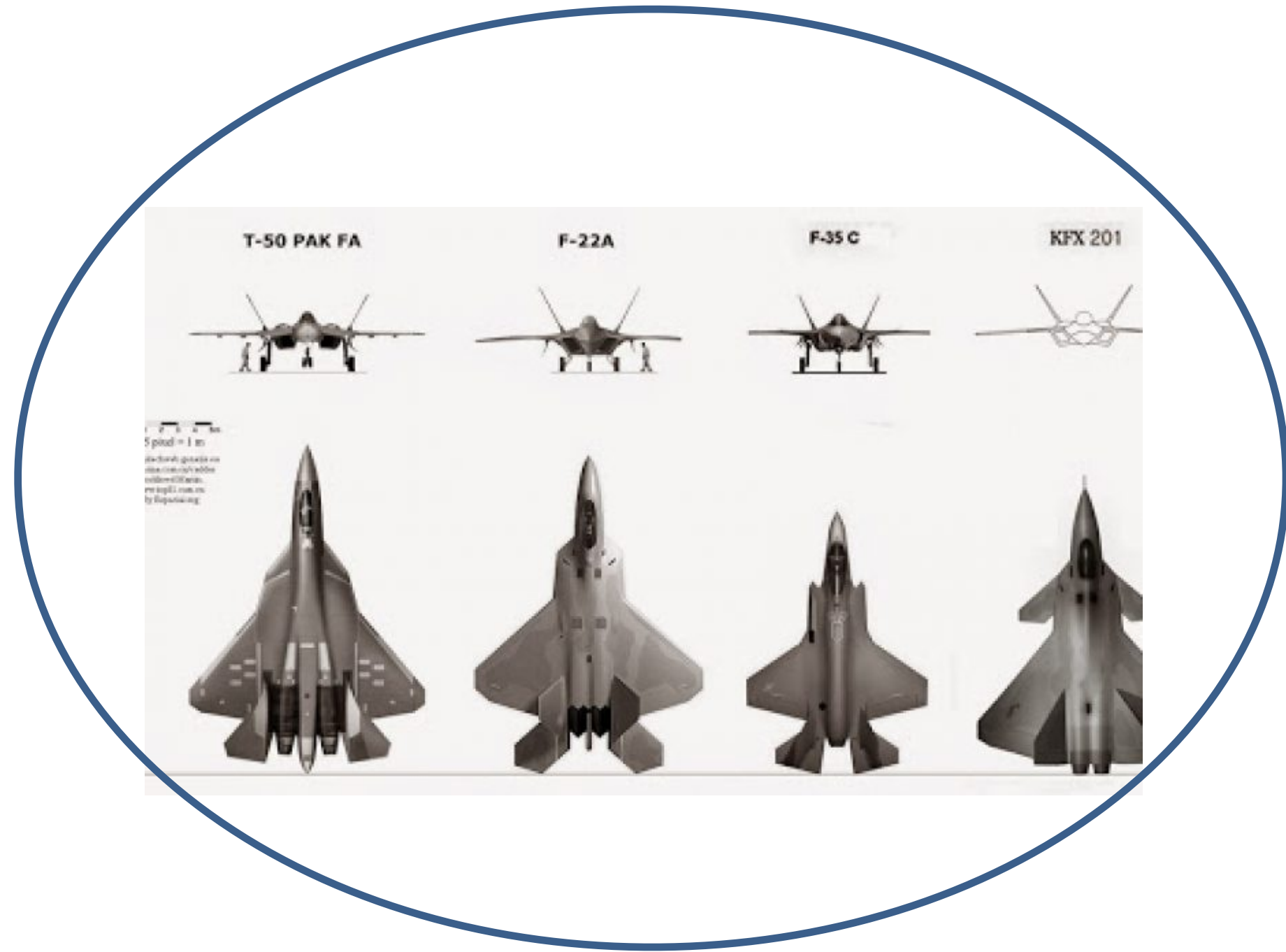


Lockheed Martin

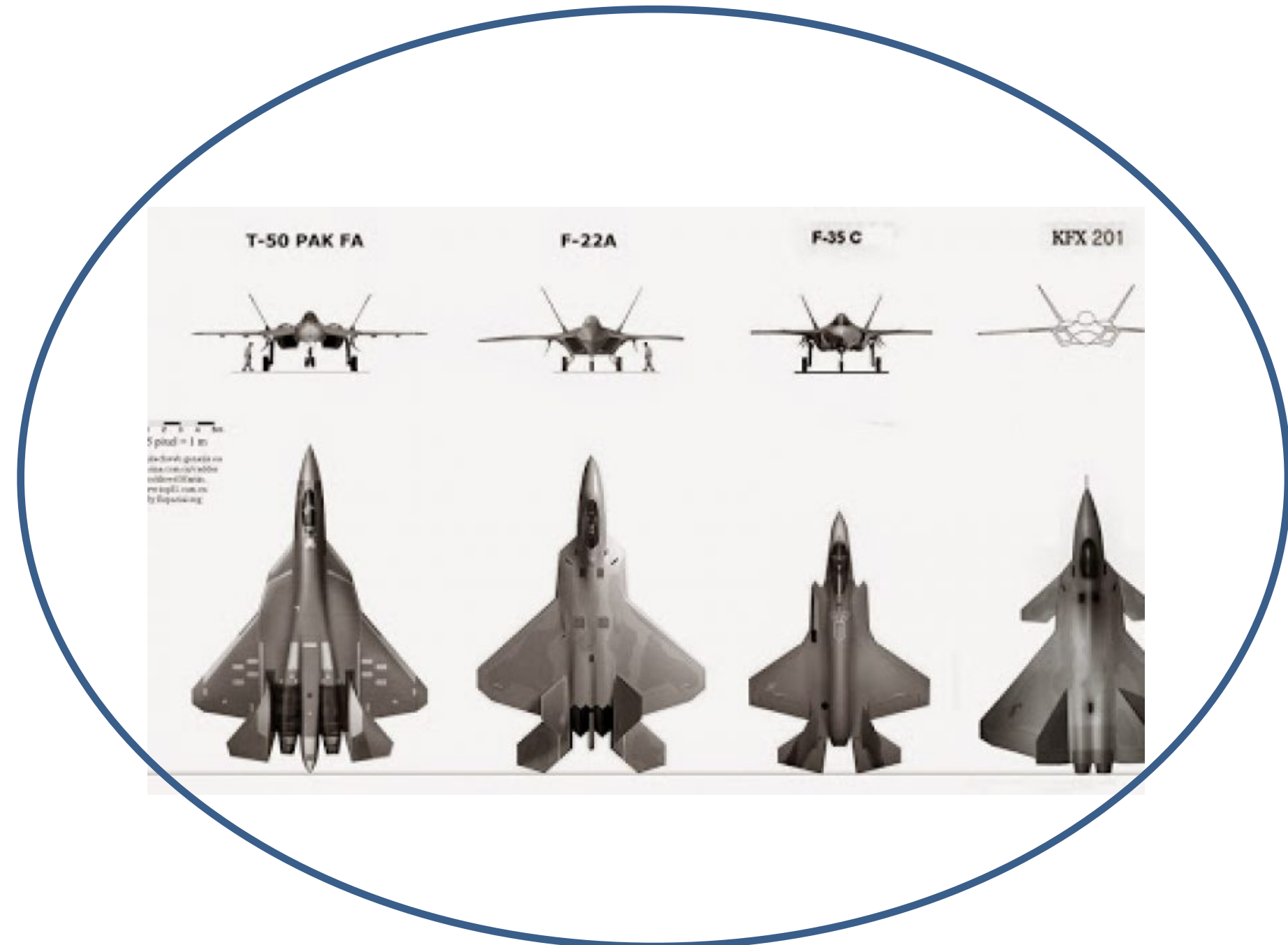
# Lockheed Martin



# Lockheed Martin

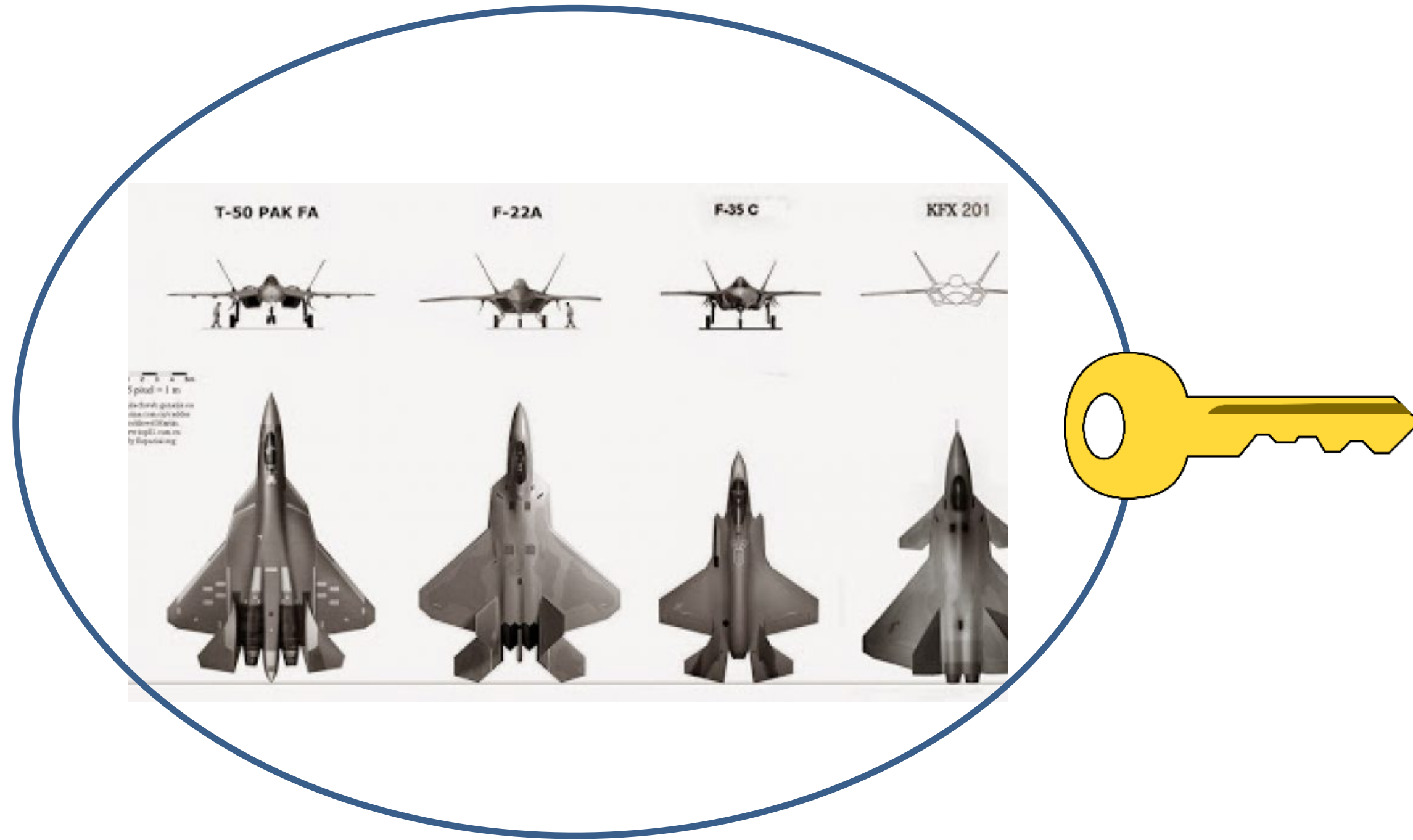


# Lockheed Martin

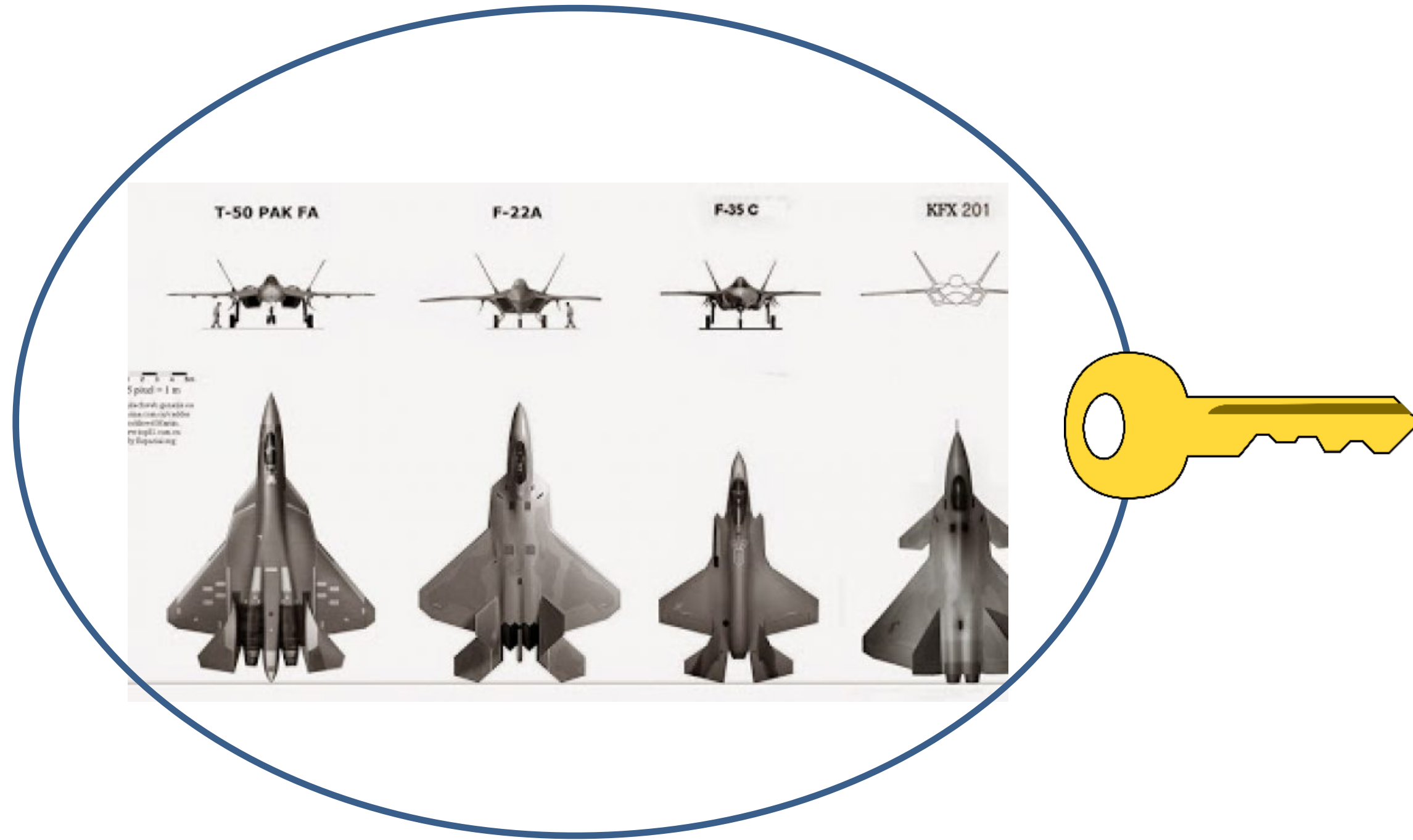




# Lockheed Martin

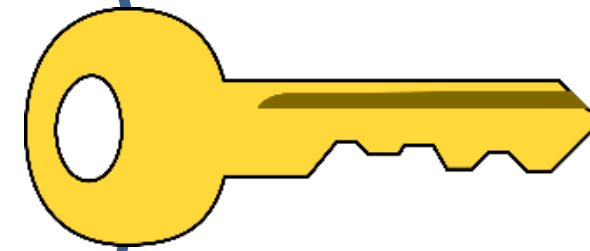


# Lockheed Martin



# Lockheed Martin

Hackers stole data on Pentagon's newest fighter jet

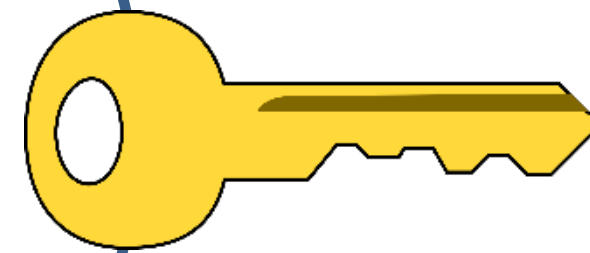


# Lockheed Martin

Defense Contractor Lockheed Martin Gets Hacked



Hackers stole data on Pentagon's newest fighter jet

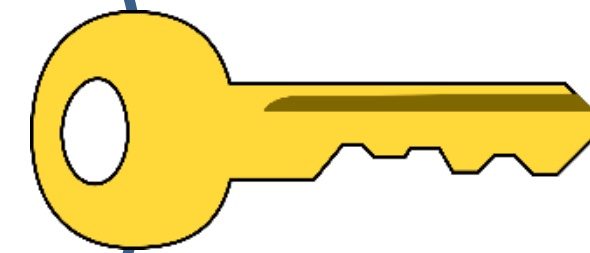


# Lockheed Martin

Defense Contractor Lockheed Martin Gets Hacked



Hackers stole data on Pentagon's newest fighter jet



## New Snowden Documents Reveal Chinese Behind F-35 Hack

Experts have long argued that China has copied the F-35 design for its own fighter jets. Is this the proof?

By Franz-Stefan Gady  
January 27, 2015



LOCKHEED

# Lockheed Martin



# Lockheed Martin

- In 2011 Lockheed Martin was hacked



# Lockheed Martin

- In 2011 Lockheed Martin was hacked
- F35 design plans were stolen





# Lockheed Martin

- In 2011 Lockheed Martin was hacked
- F35 design plans were stolen
- The attackers initially hacked RSA security



# Lockheed Martin

- In 2011 Lockheed Martin was hacked
- F35 design plans were stolen
- The attackers initially hacked RSA security
- Sent phishing emails to 2 groups



# Lockheed Martin

- In 2011 Lockheed Martin was hacked
- F35 design plans were stolen
- The attackers initially hacked RSA security
- Sent phishing emails to 2 groups
- Subject line “2011 Recruitment Plan”



# Lockheed Martin

- In 2011 Lockheed Martin was hacked
- F35 design plans were stolen
- The attackers initially hacked RSA security
- Sent phishing emails to 2 groups
- Subject line “2011 Recruitment Plan”
- One employee retrieved the mail from the junk folder and opened the Excel file



# Lockheed Martin

- In 2011 Lockheed Martin was hacked
- F35 design plans were stolen
- The attackers initially hacked RSA security
- Sent phishing emails to 2 groups
- Subject line “2011 Recruitment Plan”
- One employee retrieved the mail from the junk folder and opened the Excel file
- The Excel file contained a malware that exploited a zero-day vulnerability in Adobe Flash to install a backdoor



Mia Ash

# Mia Ash



## Mia Ash

500+  
connections

Photographer at Mia's Photography

London, Greater London, United Kingdom | Photography

Current	Mia's Photography
Previous	Loft Studios, Clapham Studios
Education	Goldsmiths, University of London

# Mia Ash



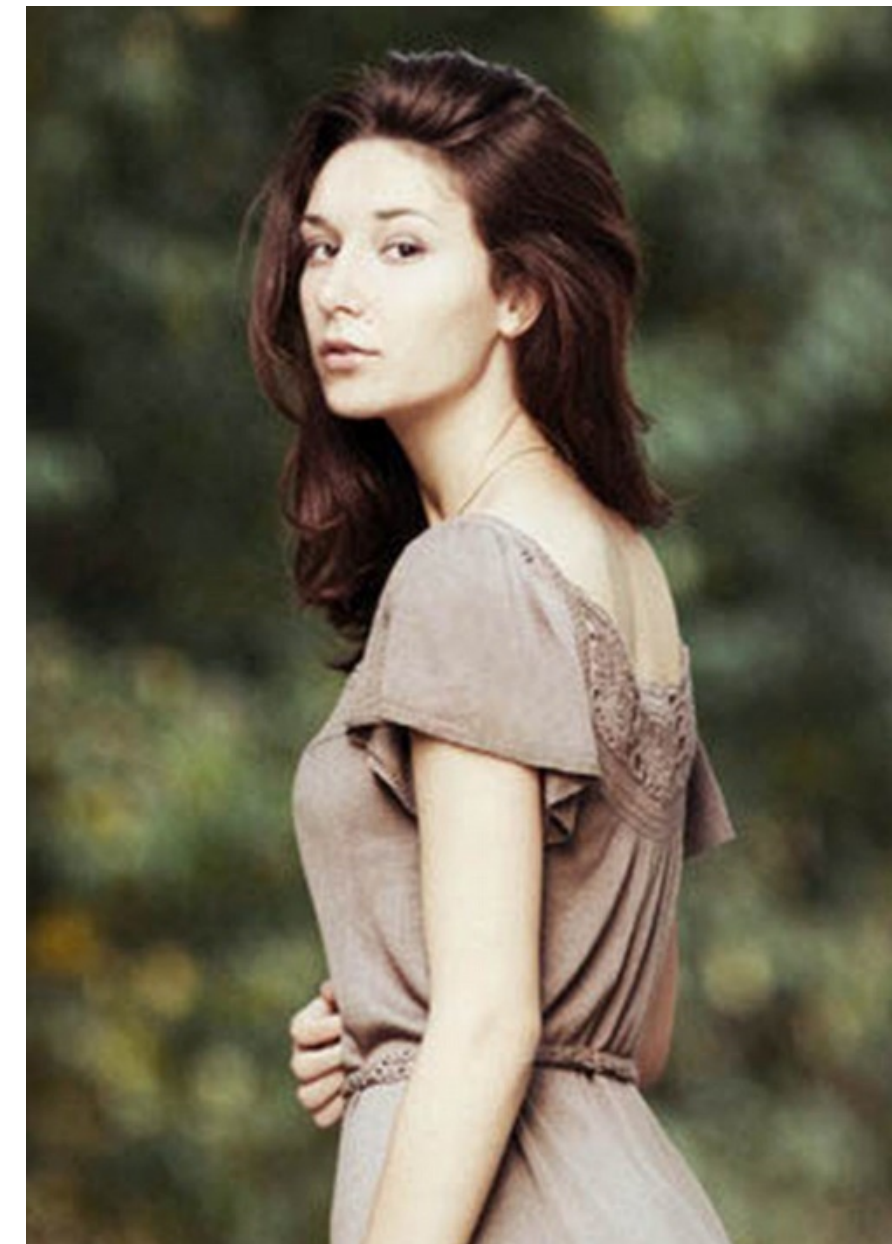
## Mia Ash

500+  
connections

Photographer at Mia's Photography

London, Greater London, United Kingdom | Photography

Current	Mia's Photography
Previous	Loft Studios, Clapham Studios
Education	Goldsmiths, University of London




Timeline

About



# Mia Ash

- 30-year-old British woman



**Mia Ash**  
Photographer at Mia's Photography  
London, Greater London, United Kingdom | Photography


500+ connections

Current	Mia's Photography
Previous	Loft Studios, Clapham Studios
Education	Goldsmiths, University of London



# Mia Ash

- 30-year-old British woman
- Two art school degrees



**Mia Ash**  
Photographer at Mia's Photography  
London, Greater London, United Kingdom | Photography


500+ connections

Current	Mia's Photography
Previous	Loft Studios, Clapham Studios
Education	Goldsmiths, University of London



# Mia Ash

- 30-year-old British woman
- Two art school degrees
- Successful career as a photographer



**Mia Ash**  
Photographer at Mia's Photography  
London, Greater London, United Kingdom | Photography

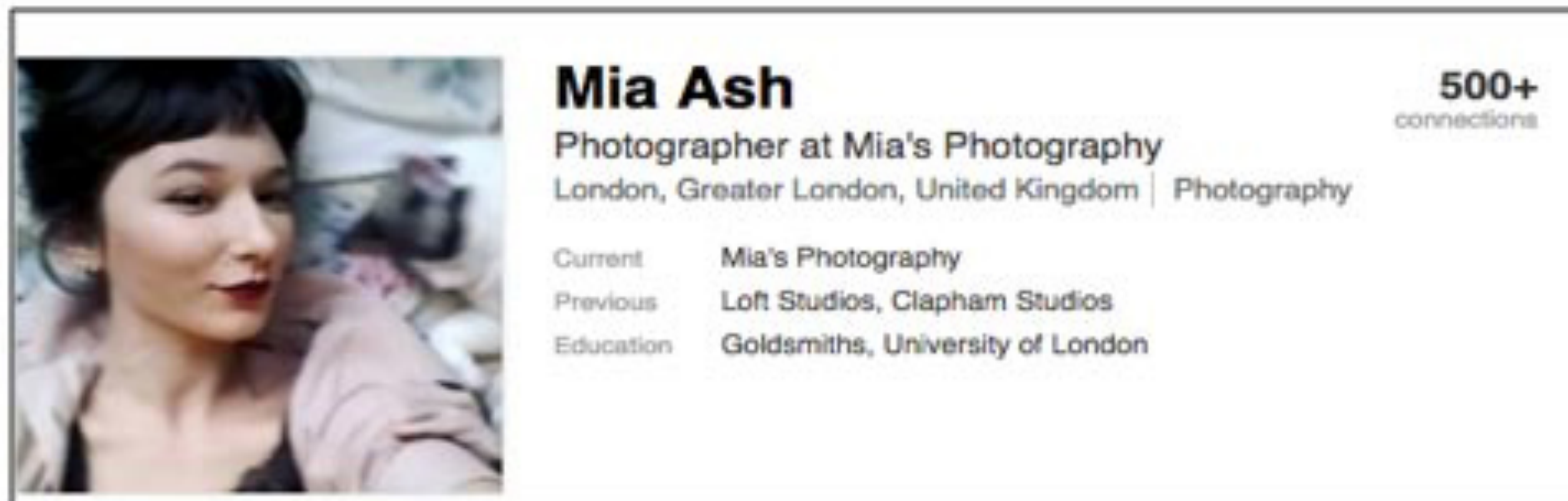
500+ connections

Current	Mia's Photography
Previous	Loft Studios, Clapham Studios
Education	Goldsmiths, University of London



# Mia Ash

- 30-year-old British woman
- Two art school degrees
- Successful career as a photographer
- 500+ friends on LinkedIn (many known photographers)



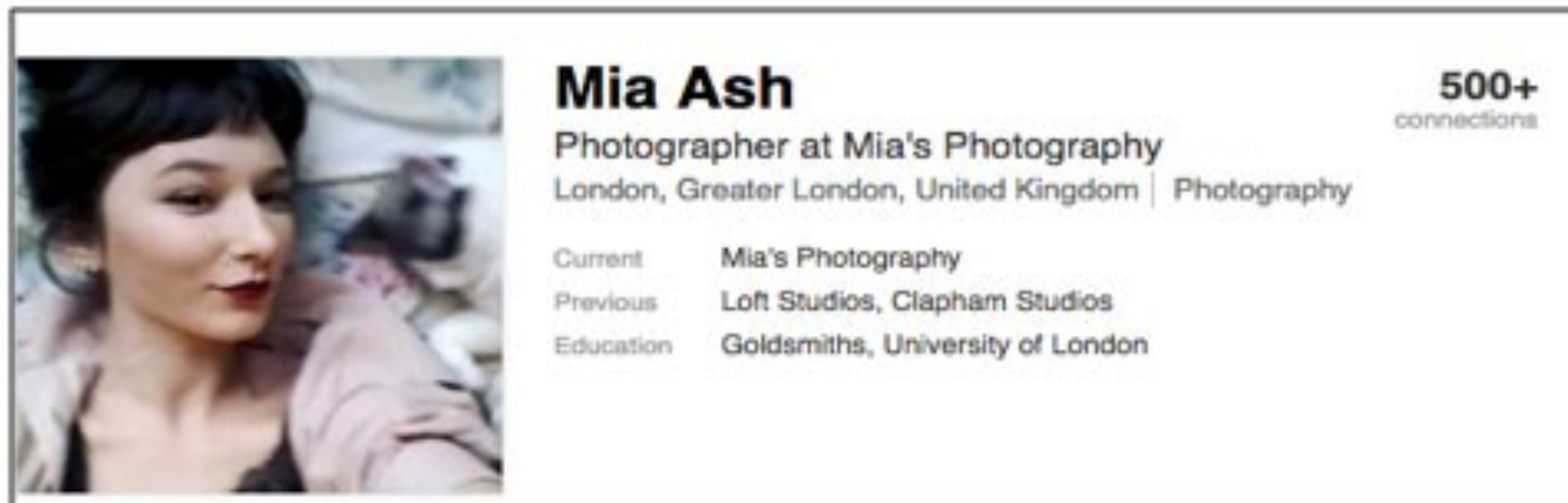
**Mia Ash** 500+ connections  
Photographer at Mia's Photography  
London, Greater London, United Kingdom | Photography

Current	Mia's Photography
Previous	Loft Studios, Clapham Studios
Education	Goldsmiths, University of London



# Mia Ash

- 30-year-old British woman
- Two art school degrees
- Successful career as a photographer
- 500+ friends on LinkedIn (many known photographers)
- Active Instagram/Facebook accounts



**Mia Ash**  
500+ connections

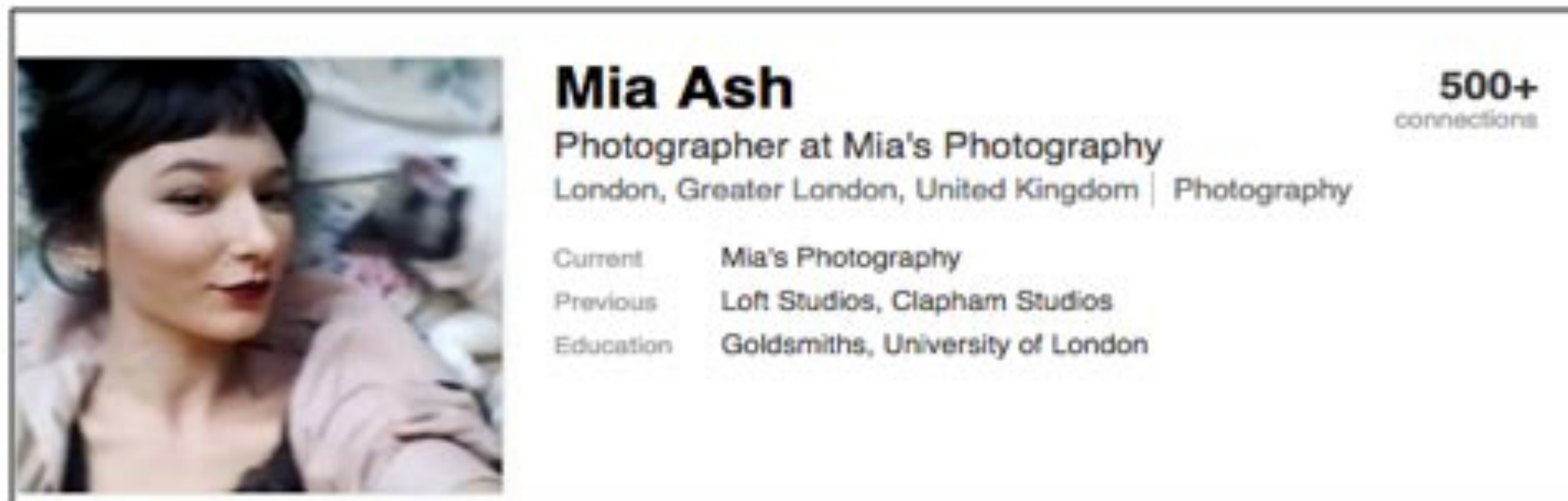
Photographer at Mia's Photography  
London, Greater London, United Kingdom | Photography

Current	Mia's Photography
Previous	Loft Studios, Clapham Studios
Education	Goldsmiths, University of London



# Mia Ash

- 30-year-old British woman
- Two art school degrees
- Successful career as a photographer
- 500+ friends on LinkedIn (many known photographers)
- Active Instagram/Facebook accounts
- Relationship status: 'It's complicated'



**Mia Ash**  
500+ connections

Photographer at Mia's Photography  
London, Greater London, United Kingdom | Photography

Current	Mia's Photography
Previous	Loft Studios, Clapham Studios
Education	Goldsmiths, University of London



Mia Ash

# Mia Ash

- In Dec 2016 – Jan 2017 there were phishing attacks targeting Middle East companies



# Mia Ash

- In Dec 2016 – Jan 2017 there were phishing attacks targeting Middle East companies
- Trying to inject PupyRAT (Remote Access Trojan)

# Mia Ash

- In Dec 2016 – Jan 2017 there were phishing attacks targeting Middle East companies
- Trying to inject PupyRAT (Remote Access Trojan)
- The phishing attack was unsuccessful

# Mia Ash

- In Dec 2016 – Jan 2017 there were phishing attacks targeting Middle East companies
- Trying to inject PupyRAT (Remote Access Trojan)
- The phishing attack was unsuccessful
- Iranian hackers (Cobalt Gypsy) created a fake virtual entity: Mia Ash

# Mia Ash

- In Dec 2016 – Jan 2017 there were phishing attacks targeting Middle East companies
- Trying to inject PupyRAT (Remote Access Trojan)
- The phishing attack was unsuccessful
- Iranian hackers (Cobalt Gypsy) created a fake virtual entity: Mia Ash
- Jan 13, Mia Ash contacted an employee via LinkedIn

# Mia Ash

- In Dec 2016 – Jan 2017 there were phishing attacks targeting Middle East companies
- Trying to inject PupyRAT (Remote Access Trojan)
- The phishing attack was unsuccessful
- Iranian hackers (Cobalt Gypsy) created a fake virtual entity: Mia Ash
- Jan 13, Mia Ash contacted an employee via LinkedIn
- Jan 21, Mia asked to continue Facebook

# Mia Ash

- In Dec 2016 – Jan 2017 there were phishing attacks targeting Middle East companies
- Trying to inject PupyRAT (Remote Access Trojan)
- The phishing attack was unsuccessful
- Iranian hackers (Cobalt Gypsy) created a fake virtual entity: Mia Ash
- Jan 13, Mia Ash contacted an employee via LinkedIn
- Jan 21, Mia asked to continue Facebook
- Correspondence continues via email/WhatsApp/Facebook

# Mia Ash

- In Dec 2016 – Jan 2017 there were phishing attacks targeting Middle East companies
- Trying to inject PupyRAT (Remote Access Trojan)
- The phishing attack was unsuccessful
- Iranian hackers (Cobalt Gypsy) created a fake virtual entity: Mia Ash
- Jan 13, Mia Ash contacted an employee via LinkedIn
- Jan 21, Mia asked to continue Facebook
- Correspondence continues via email/WhatsApp/Facebook
- Feb 12 Mia emailed 'Copy of Photography Survey.xlsx'

# Mia Ash

- In Dec 2016 – Jan 2017 there were phishing attacks targeting Middle East companies
- Trying to inject PupyRAT (Remote Access Trojan)
- The phishing attack was unsuccessful
- Iranian hackers (Cobalt Gypsy) created a fake virtual entity: Mia Ash
- Jan 13, Mia Ash contacted an employee via LinkedIn
- Jan 21, Mia asked to continue Facebook
- Correspondence continues via email/WhatsApp/Facebook
- Feb 12 Mia emailed 'Copy of Photography Survey.xlsm'
- Mia encouraged to open the email at work using corporate email account



# Mia Ash

- In Dec 2016 – Jan 2017 there were phishing attacks targeting Middle East companies
- Trying to inject PupyRAT (Remote Access Trojan)
- The phishing attack was unsuccessful
- Iranian hackers (Cobalt Gypsy) created a fake virtual entity: Mia Ash
- Jan 13, Mia Ash contacted an employee via LinkedIn
- Jan 21, Mia asked to continue Facebook
- Correspondence continues via email/WhatsApp/Facebook
- Feb 12 Mia emailed 'Copy of Photography Survey.xlsm'
- Mia encouraged to open the email at work using corporate email account
- The Excel file contained a macro that downloaded PupyRAT


Mia Ash

# Mia Ash

- Most content taken from other accounts

# Mia Ash

- Most content taken from other accounts



**Mia Ash**  
Photographer at Mia's Photography  
London, Greater London, United Kingdom | Photography

500+ connections

Current	Mia's Photography
Previous	Loft Studios, Clapham Studios
Education	Goldsmiths, University of London



bittersweetvenom24 [Follow](#)

147 views 23w

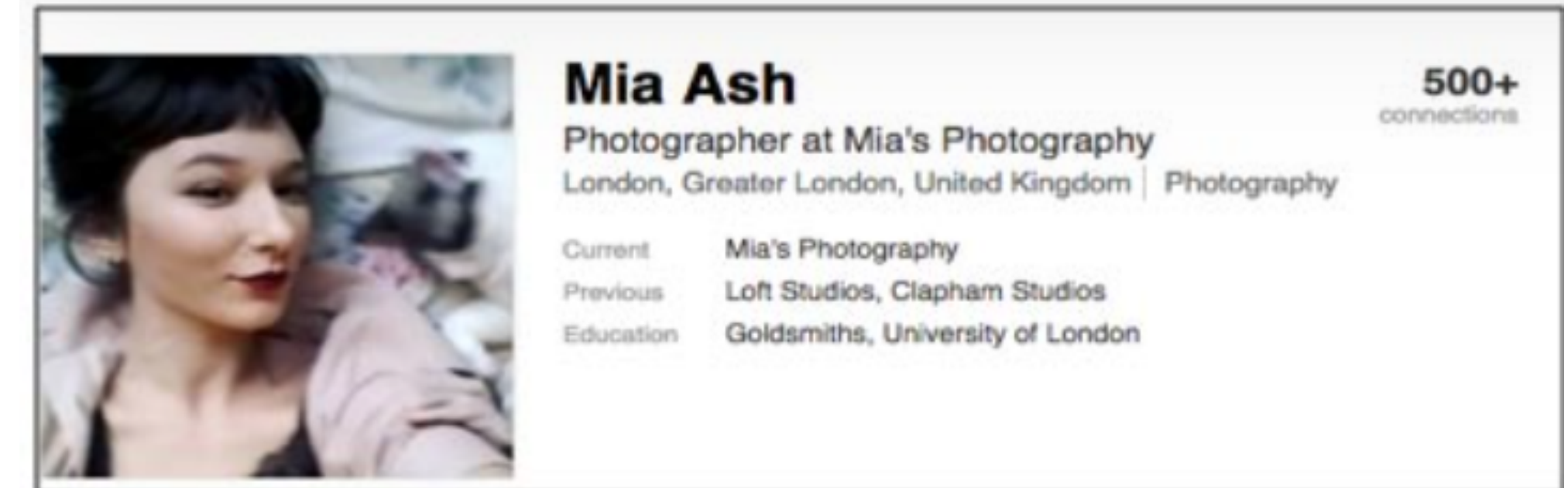
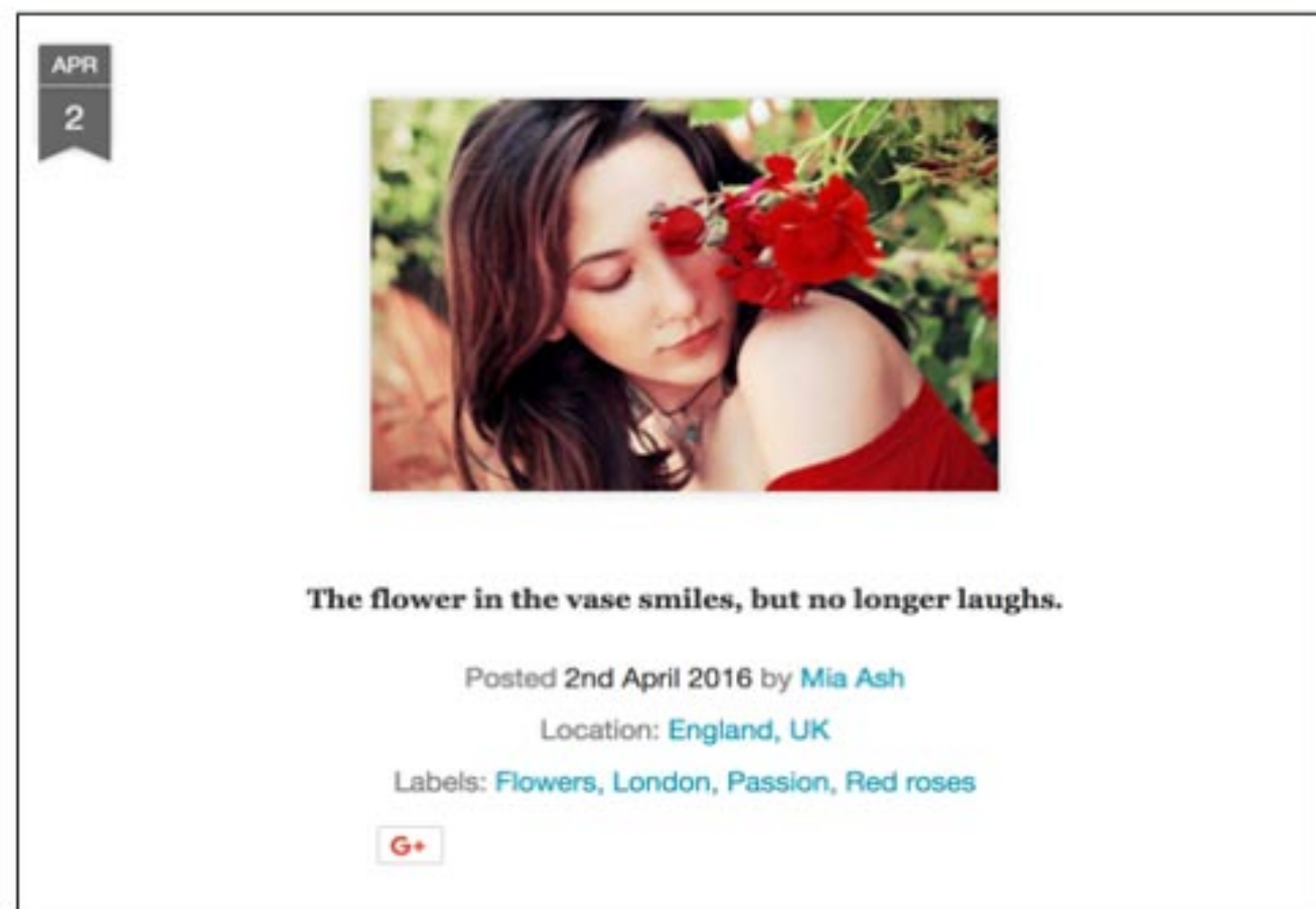
bittersweetvenom24 Jbam!  
[#oscarthefatcat](#) [#oscarthecat](#) [#sleepingcat](#)  
[#aww](#) [#boomerang](#)

Log in to like or comment.

<https://www.instagram.com/>

# Mia Ash

- Most content taken from other accounts



<https://www.instagram.com/>

# Mia Ash

- Mia's job description is almost identical to an account of a U.S.-based photographer

# Mia Ash

- Mia's job description is almost identical to an account of a U.S.-based photographer

## **Photographer**

Mia's Photography

January 2014 – Present (3 years 3 months) | London, United Kingdom

- Lead editor for numerous books, gallery shows, and images for media and multimedia broadcasts
- Consulted as photo editor for various International shows
- Implemented processes and structure for digital archiving, trafficked imagery, and conducted photo research and photo editing for publishing, multimedia, and exhibition projects
- Secured digital image submissions and prepared digital image priming and prepress for multi-platform projects
- Managed writing image use, photographer agreement contracts, and negotiated licensing terms and fees

## **Manager, Photo Editing + Image Collection + Special Projects**

International League of Conservation Photographers

2009 – 2010 • 1 yr

- Lead editor for numerous books, gallery shows, and images for media and multimedia broadcasts
- Selected to edit a Christies Auction House gallery of "Best Nature Photographs of All Time"
- Consulted as photo editor for Conservation International
- Implemented processes and structure for digital archiving, trafficked imagery, and conducted photo research and photo editing for publishing, multimedia, and exhibition projects such as "Freshwater: The Essence of Life"
- Secured digital image submissions and prepared digital image priming and prepress for multiplatform projects
- Managed writing image use, photographer agreement contracts, and negotiated licensing terms and fees

# Mia Ash

- Mia's job description is almost identical to an account of a U.S.-based photographer

## **Photographer**

Mia's Photography

January 2014 – Present (3 years 3 months) | London, United Kingdom

- Lead editor for numerous books, gallery shows, and images for media and multimedia broadcasts
- Consulted as photo editor for various International shows
- Implemented processes and structure for digital archiving, trafficked imagery, and conducted photo research and photo editing for publishing, multimedia, and exhibition projects
- Secured digital image submissions and prepared digital image priming and prepress for multi-platform projects
- Managed writing image use, photographer agreement contracts, and negotiated licensing terms and fees

## **Manager, Photo Editing + Image Collection + Special Projects**

International League of Conservation Photographers

2009 – 2010 • 1 yr

- Lead editor for numerous books, gallery shows, and images for media and multimedia broadcasts
- Selected to edit a Christies Auction House gallery of "Best Nature Photographs of All Time"
- Consulted as photo editor for Conservation International
- Implemented processes and structure for digital archiving, trafficked imagery, and conducted photo research and photo editing for publishing, multimedia, and exhibition projects such as "Freshwater: The Essence of Life"
- Secured digital image submissions and prepared digital image priming and prepress for multiplatform projects
- Managed writing image use, photographer agreement contracts, and negotiated licensing terms and fees

<https://www.secureworks.com/research/the-curious-case-of-mia-ash>



# Robin Sage



# Robin Sage

- A virtual entity created in 2009 by Robin Casey and Thomas Ryan (Black Hat 2010)



# Robin Sage

- A virtual entity created in 2009 by Robin Casey and Thomas Ryan (Black Hat 2010)
- 25-year-old 'cyber threat analyst'



# Robin Sage

- A virtual entity created in 2009 by Robin Casey and Thomas Ryan (Black Hat 2010)
- 25-year-old 'cyber threat analyst'
- MIT graduate



# Robin Sage

- A virtual entity created in 2009 by Robin Casey and Thomas Ryan (Black Hat 2010)
- 25-year-old 'cyber threat analyst'
- MIT graduate
- Works at Naval Network Warfare Command in Norfolk, Virginia



# Robin Sage

- A virtual entity created in 2009 by Robin Casey and Thomas Ryan (Black Hat 2010)
- 25-year-old 'cyber threat analyst'
- MIT graduate
- Works at Naval Network Warfare Command in Norfolk, Virginia
- Has 10 years of work experience



# Robin Sage

- A virtual entity created in 2009 by Robin Casey and Thomas Ryan (Black Hat 2010)
- 25-year-old 'cyber threat analyst'
- MIT graduate
- Works at Naval Network Warfare Command in Norfolk, Virginia
- Has 10 years of work experience
- Facebook/LinkedIn/Twitter accounts



# Robin Sage

- A virtual entity created in 2009 by Robin Casey and Thomas Ryan (Black Hat 2010)
- 25-year-old 'cyber threat analyst'
- MIT graduate
- Works at Naval Network Warfare Command in Norfolk, Virginia
- Has 10 years of work experience
- Facebook/LinkedIn/Twitter accounts
- Offered consulting work with Google and Lockheed Martin





# Robin Sage

- A virtual entity created in 2009 by Robin Casey and Thomas Ryan (Black Hat 2010)
- 25-year-old 'cyber threat analyst'
- MIT graduate
- Works at Naval Network Warfare Command in Norfolk, Virginia
- Has 10 years of work experience
- Facebook/LinkedIn/Twitter accounts
- Offered consulting work with Google and Lockheed Martin
- Received dinner invitations from several male contacts



# Robin Sage



I wanted to Thank those  
of you who offered me  
dinner. Where are we  
going tonight?



<https://www.youtube.com/watch?v=4pnKbibi6QY>