

# GameSS

PHISHING



# WHO IS THE MATERIAL FOR?

This material will provide introduction into phishing attacks and countermeasures. It is suitable for a broad range of target groups, such as developers, admins, employees and managers.



# WHO MADE THIS MATERIAL?

Oksana Kulyk

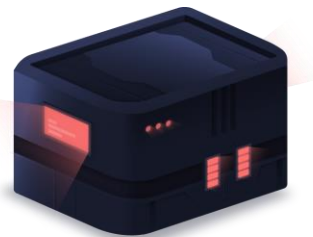
Associate Professor at IT University of Copenhagen (ITU)

[okku@itu.dk](mailto:okku@itu.dk)



# WHAT ARE THE MAIN TAKEAWAYS FOR THIS CONTENT?

- Phishing is a social engineering attack involving impersonation of a trusted entity via email and other remote communication channels. Spear phishing is a targeted variant of the attack.
- Attackers use a variety of tactics to compose phishing emails, in particular, different methods of impersonating the sender and hiding the URL of the phishing website.
- Phishing emails can be detected with automatic and manual inspection, both of which have their strengths and limitations
- Anti-phishing education is challenging to implement correctly and should not be relied on as a sole method of preventing phishing
- A layered approach is recommended for protectiong against phishing



**Disclaimer:** the tools and techniques in this learning module are described for educational purposes only, so that you can be aware of them to better protect yourself or your company. Using them in real world on targets that don't give you permission to do so can be highly unethical and lead to legal repercussions.



# WHAT IS PHISHING

- A variant of social engineering attack
- Attacker sends emails (or messages via other channels, e.g. SMS) impersonating a trusted entity

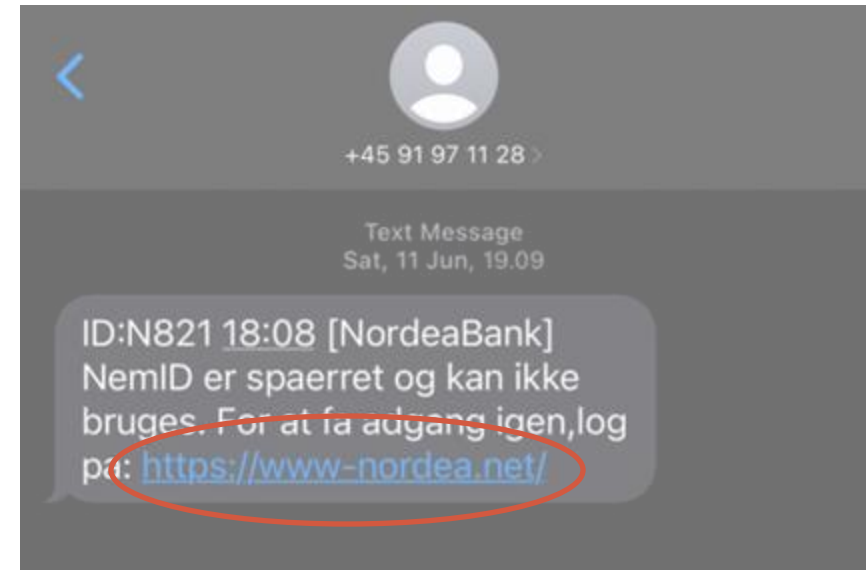
→ How can one tell this is not a real message from Nordea?



# WHAT IS PHISHING

→ How can one tell this is not a real message from Nordea?

- Main indicator: link does not lead to the Nordea website
- Other possible indicators
  - Time of message: Saturday evening
  - Spelling mistakes
  - Content invoking sense of urgency



# PHISHING IS WIDE-SPREAD

Oplevet it-kriminalitet i forbindelse med privat brug af internet inden for det seneste år. 2019



Kilde: [www.statistikbanken.dk/bebrit19](http://www.statistikbanken.dk/bebrit19).





# GOAL: STEAL SENSITIVE INFORMATION

CYBERSECURITY

## How the Russians broke into the Democrats' email, and how it could have been avoided

PUBLISHED MON, JUL 16 2018·11:15 AM EDT | UPDATED TUE, JUL 17 2018·AT 11:13 EDT

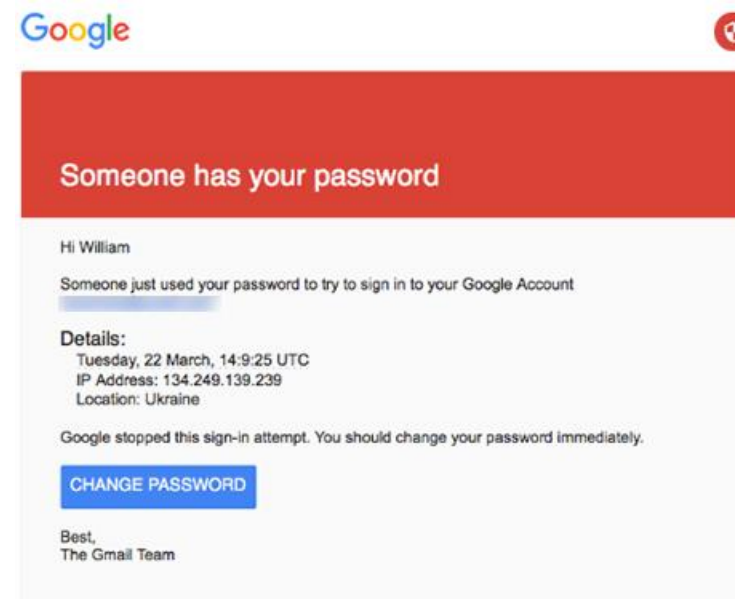


Kate Fazzini  
@KATEFAZZINI

SHARE [f](#) [t](#) [in](#) [✉](#)

According to the Justice Department, the Russians used spear-phishing as one of their primary attack techniques. Spear-phishing refers to an email targeted at an important person — or a “big fish” — who can provide entry to a cache of the most important data. It starts with basic reconnaissance (like looking at [Facebook](#) <sup>+</sup> and [LinkedIn](#) <sup>+</sup> profiles) to create a portrait of a prominent individual, then using that portrait to create an email that he or she is sure to click on. In the Democratic National Committee hack in 2016, those emails were just spoofed to look like security updates from Google, according to the indictment.

Source: CNBS



You received this mandatory email service announcement to update you about important changes to your Google product or account.

Source: Ars Technica



# GOAL: IMPERSONATE SPECIFIC PEOPLE

TECH \ TWITTER \ CYBERSECURITY \

## Twitter says a spear phishing attack led to the huge bitcoin scam

*'This attack relied on a significant and concerted attempt to mislead certain employees'*

By Jay Peters | @jaypeters | Jul 30, 2020, 9:29pm EDT

Source: TheVerge

### What we know now

The social engineering that occurred on July 15, 2020, targeted a small number of employees through a phone spear phishing attack. A successful attack required the attackers to obtain access to both our internal network as well as specific employee credentials that granted them access to our internal support tools. Not all of the employees that were initially targeted had permissions to use account management tools, but the attackers used their credentials to access our internal systems and gain information about our processes. This knowledge then enabled them to target additional employees who did have access to our account support tools. Using the credentials of employees with access to these tools, the attackers targeted 130 Twitter accounts, ultimately Tweeting from 45, accessing the DM inbox of 36, and downloading the Twitter Data of 7.

 Tweet

Source: Twitter blog



# GOAL: CONDUCT UNAUTHORISED OPERATIONS

## The Lazarus heist: How North Korea almost pulled off a billion-dollar hack

🕒 21 June 2021


In January 2015, an innocuous-looking email had been sent to several Bangladesh Bank employees. It came from a job seeker calling himself Rasel Ahlam. His polite enquiry included an invitation to download his CV and cover letter from a website. In reality, Rasel did not exist - he was simply a cover name being used by the Lazarus Group, according to FBI investigators. At least one person inside the bank fell for the trick, downloaded the documents, and got infected with the viruses hidden inside.


Once inside the bank's systems, Lazarus Group began stealthily hopping from computer to computer, working their way towards the digital vaults and the billions of dollars they contained.

Source: BBC

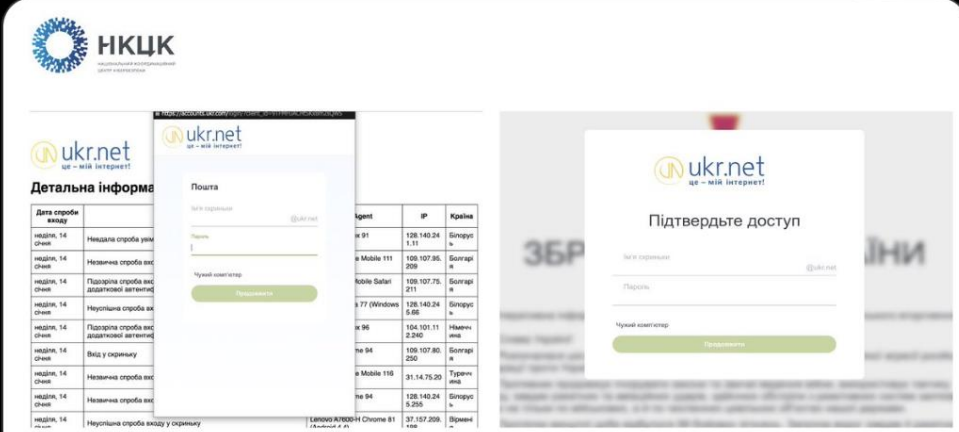


# GOAL: INFILTRATE MILITARY INFRASTRUCTURE

 **НКЦК** @ncscUA · Jan 27

 russian group APT28 conducts phishing attacks against Ukrainian military personnel.

#APT28 is distributing phishing html pages of the ukr[.]net mail service and is aimed at gaining access to the mailboxes of military personnel and units of the Ukrainian Defence Forces.



The image displays three screenshots of phishing pages for ukr.net. The leftmost screenshot shows a 'Детальна інформація' (Detailed information) page with a table of activity logs. The middle screenshot shows a 'Пошта' (Mail) login page with fields for 'Почта' and 'Чувий код/клар' (Security code/ID). The rightmost screenshot shows a 'Підтвердьте доступ' (Confirm access) page with a 'Почта' field and a 'Чувий код/клар' field. Below the screenshots is a table of IP addresses and their corresponding countries.

Agent	IP	Країна
91	128.140.24.131	Білорусія
Mobile 111	106.107.96.209	Бразилія
Mobile Safari	106.107.75.211	Бразилія
77 (Windows)	128.140.24.95	Білорусія
96	104.101.11.234	Нідерланди
94	106.107.80.250	Бразилія
Mobile 118	31.14.75.29	Туреччина
94	128.140.24.95	Білорусія
37.157.209	37.157.209	Вірменія

**RUSSIAN GROUP APT28 CONDUCTS PHISHING ATTACKS AGAINST UKRAINIAN MILITARY PERSONNEL**

Source: Ukraine National Cyber Security Coordination Center

# HOW PHISHING WORKS: CREDENTIALS STEALING

1. User get an email with a link to a website of a trusted organisation
2. The link goes to the website that looks like the one from the real organisation but is owned by the attacker
3. User is prompted to enter credentials
4. Credentials forwarded to the attacker
5. Attacker gets full control over user's account



# HOW PHISHING WORKS: MALWARE INFILTRATION

1. User gets an email with an attached file
2. User opens the attachment in the email
3. Attachment runs malware script
4. Malware gets control over the users' system (e.g. sending data to the attacker) and/or propagates to other users/devices on the network
5. In rare cases: malware can run even without the user opening the file: clicking the link, or even just reading the email → especially dangerous for systems without security updates



# HOW PHISHING WORKS: CEO FRAUD

1. User gets an email impersonating a trusted person/authority
2. The email contains instructions: transferring money, sharing sensitive documents...
3. User follows the instructions



# HOW HARD IS PHISHING: REGULAR PHISHING

- Attacker's investment:
  - Register email addresses to use for phishing mailing
  - Register a website to make it look like the one the attacker wants to impersonate, or:
  - Prepare malware to be attached
  - Send out phishing emails
- Openly available tools incl. generative AI exist to help

```
Select from the menu:  
  
1) Spear-Phishing Attack Vectors  
2) Website Attack Vectors  
3) Infectious Media Generator  
4) Create a Payload and Listener  
5) Mass Mailer Attack  
6) Arduino-Based Attack Vector  
7) Wireless Access Point Attack Vector  
8) QRCode Generator Attack Vector  
9) Powershell Attack Vectors  
10) Third Party Modules  
  
99) Return back to the main menu.  
  
set> |
```

Source: Social Engineering Toolkit

## After WormGPT, FraudGPT Emerges to Help Scammers Steal Your Data

The arrival of WormGPT and now FraudGPT signals that hackers are seizing the opportunity to create AI-powered chatbots to facilitate cybercrime and scams.

by [Michael Kan](#)  
Jul 25, 2023

[f](#) [X](#) [in](#) [P](#)

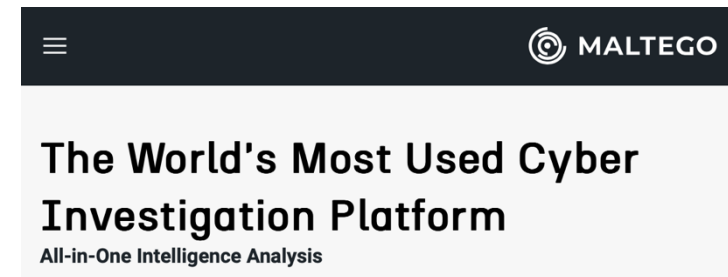
Source: PCmag





# HOW HARD IS PHISHING: SPEAR PHISHING

- Additional investment to personalise the attack
  - Identify suitable recipients (e.g. company employees)
  - Learn information about the target
    - Names of their colleagues
    - Facts about the company
    - Personal facts, e.g. recent vacation
    - ...
- Prepare a believable phishing email
- Openly available tools exist to help the investigations



```
*****
*
* theHarvester
*
* theHarvester 4.4.3
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****
usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-s START] [-p] [-s] [--screenshot SCREENSH
[-t] [-r [DNS_RESOLVE]] [-n] [-e] [-f FILENAME] [-b SOURCE]

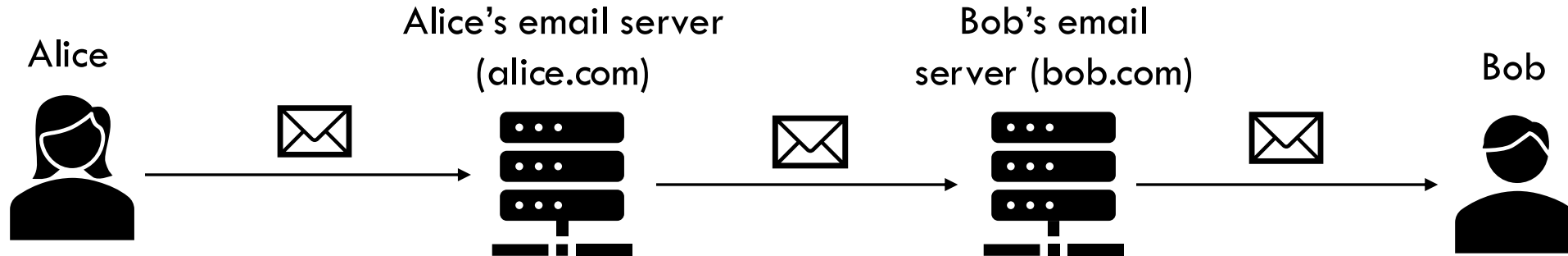
theHarvester is used to gather open source intelligence (OSINT) on a company or domain.
```





**How can phishing emails look like?**

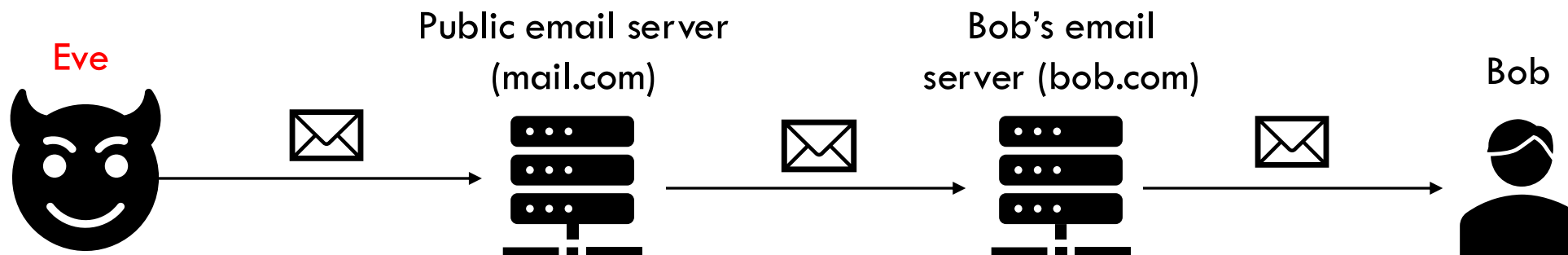
# HOW EMAIL WORKS



```
From: Alice <alice@alice.com>  
To: Bob <bob@bob.com>  
Subject: Meeting agenda
```

→ **Simple Mail Transfer Protocol**: originally designed in 1980, no initial security considerations in mind

# SENDER SPOOFING: SENDER'S NAME

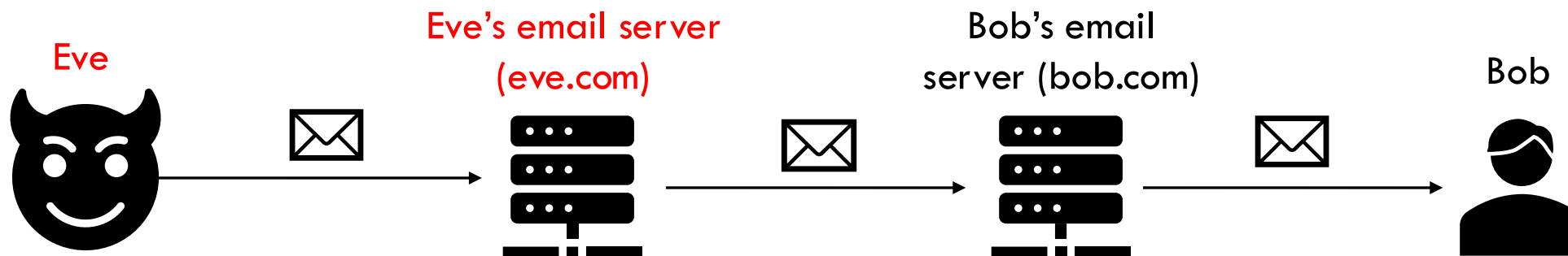


```
From: Alice <eve@mail.com>  
To: Bob <bob@bob.com>  
Subject: Meeting agenda
```

- Sender's name falsifiable
- Sender's address can look similar enough to be believable
  - "alice@mail.com" (if Alice hasn't registered the account at mail.com herself)
  - "alice@eve.com"
  - ...



# SENDER SPOOFING: SENDER'S ADDRESS



```
From: Alice <alice@alice.com>  
To: Bob <bob@bob.com>  
Subject: Meeting agenda
```

- Senders' email falsifiable if:
  - Attacker controls the server
  - or the email provider's server is incorrectly configured
- Detection measures possible → more on that later



# WEBSITE SPOOFING: HIDING THE LINK

From: YourBank <yourbank-service@mail.com>

To: Bob <bob@bob.com>

Subject: Bank account compromised

Dear Bob,

Unfortunately your bank account has been compromised and has therefore been blocked. Please go to our website following this link: <https://yourbank.com/account-restore> and enter your online banking login and password to restore the account.

- Real link destination can be hidden in email text → visible only via tooltip/hovering on the link
- Further tricks to disguise the actual URL



# WEBSITE SPOOFING: HIDING THE LINK

From: YourBank <yourbank-service@mail.com>

To: Bob <bob@bob.com>

Subject: Bank account compromised

Dear Bob,

Unfortunately your bank account has been compromised and has therefore been blocked.

Please go to our website following this link: <https://yourbank.com/account-restore> and

enter your online banking login and password to restore the <https://evilhacker.org/phishing>

- Real link destination can be hidden in email text → visible only via tooltip/hovering on the link
- Further tricks to disguise the actual URL



# TRICK 0: NO TRICK

[evilhacker.org](http://evilhacker.org)

[182.15.128.103](http://182.15.128.103)

- Should be easy to detect
- Still, the user has to pay attention to the URL





# TRICK 1: URL SHORTENERS

<https://tinyurl.com/bffte48x>

- Hard to distinguish without clicking on the link
- Services to check shortened URLs exist → need to be explicitly checked

## Unshorten.It!

Unshorten.It!

Not got a short URL to try? Here's one: <http://bit.ly/GVBQJS>

**This website does not have a title**

**Destination URL:**

<http://evilhacker.org>



## TRICK 2: LEGITIMATE WEBSITE AS PART OF URL

[amazon.com](https://amazon.com) → [amazon.com.evilhacker.com](https://amazon.com.evilhacker.com)

[facebook.com](https://facebook.com) → [evilhacker.com/www.facebook.com](https://evilhacker.com/www.facebook.com)

- A problem if user doesn't know how to identify the website domain
- A problem if only a part of URL is shown (e.g. on mobile devices)



# TRICK 3: SIMILAR DOMAINS

[amazon.com](https://amazon.com) → [amazon-shop.com](https://amazon-shop.com)

- A problem if the user does not know what the real website is



# TRICK 4: (ALMOST) INDISTINGUISHABLE DOMAINS

[amazon.com](https://amazon.com) → [arnazon.com](https://arnazon.com)

[microsoft.com](https://microsoft.com) → [mircosoft.com](https://mircosoft.com)

[facebook.com](https://facebook.com) → [fácebook.com](https://fácebook.com)

[apple.com](https://apple.com) → [apple.com](https://apple.com)

- Especially hard to notice!



# TRICK 5: COMPROMISED LEGITIMATE WEBSITES

[amazon.com](https://amazon.com) → [evilhacker.amazon.com](https://evilhacker.amazon.com)

[amazon.com](https://amazon.com) → [amazon.com/evilhacker](https://amazon.com/evilhacker)

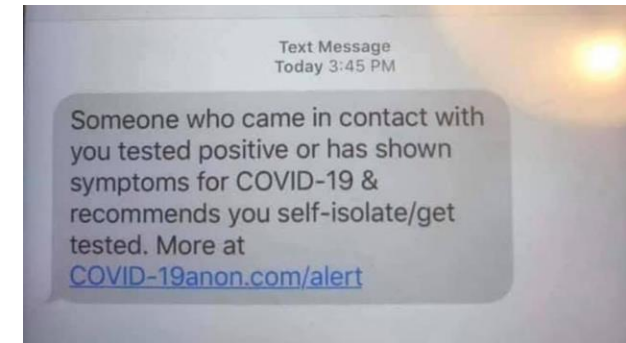
[amazon.com](https://amazon.com) → [amazon.com/login?redirect=https://evilhacker.org](https://amazon.com/login?redirect=https://evilhacker.org)

- Impossible to notice based on URL alone – website owners must take measures

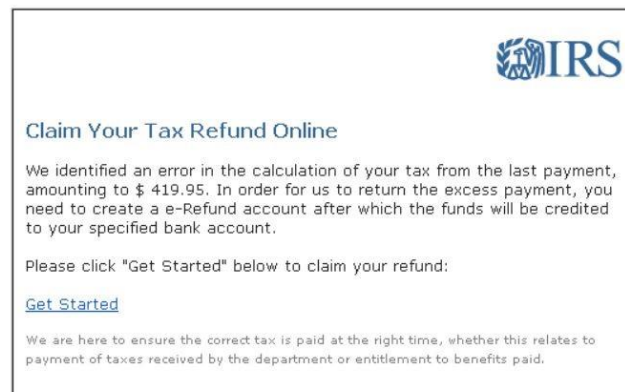


# CONTENT OF PHISHING MESSAGES

- Exploiting human psychology: fear, appeal to authority, sense of urgency, promising reward...
- Even more effective: personalisation via collecting information about the target



Source: <https://wset.com/news/coronavirus/do-not-click-the-link-police-warn-of-scam-covid-19-text-messages>



Source: <https://us.norton.com/internetsecurity-online-scams-phishing-email-examples.html>



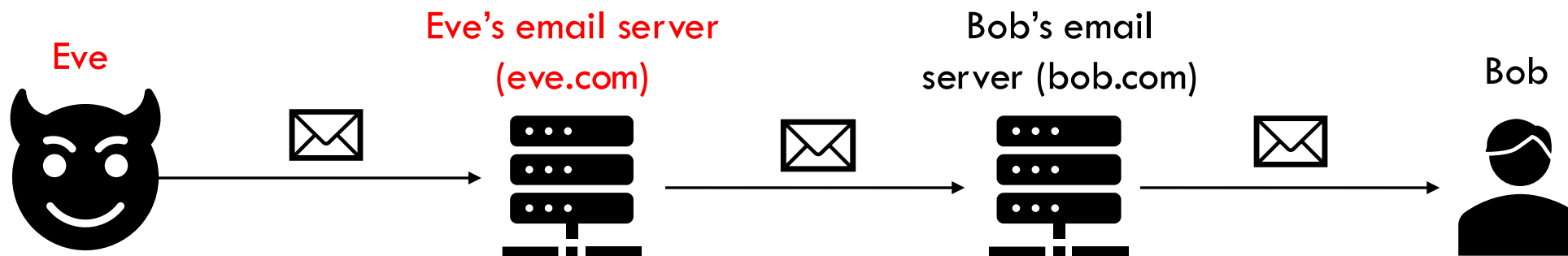
**Thomas Brewster** Forbes Staff  
Cybersecurity

Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.



# Phishing detection

# DOMAIN VERIFICATION: SENDER SPOOFING

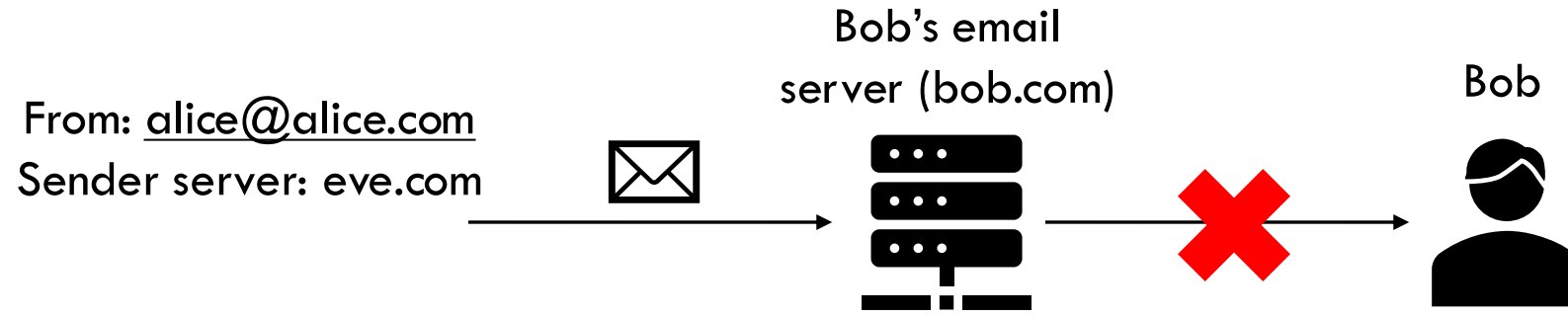


- Scenario: Eve wants to impersonate Alice
- She uses her own email server (eve.com) to spoof the sender as [alice@alice.com](mailto:alice@alice.com)
- Solution: Sender Policy Framework (SPF) record
- Idea: check with Alice's email server (alice.com) whether the server sending the email (eve.com) on Alice's behalf is actually allowed to do so
- If not:
  - either soft fail (email delivered to Bob but marked as failed verification)
  - or fail (email not delivered)





# DOMAIN VERIFICATION: SENDER POLICY FRAMEWORK



“Can the server at eve.com send emails with a sender from alice.com?”

No

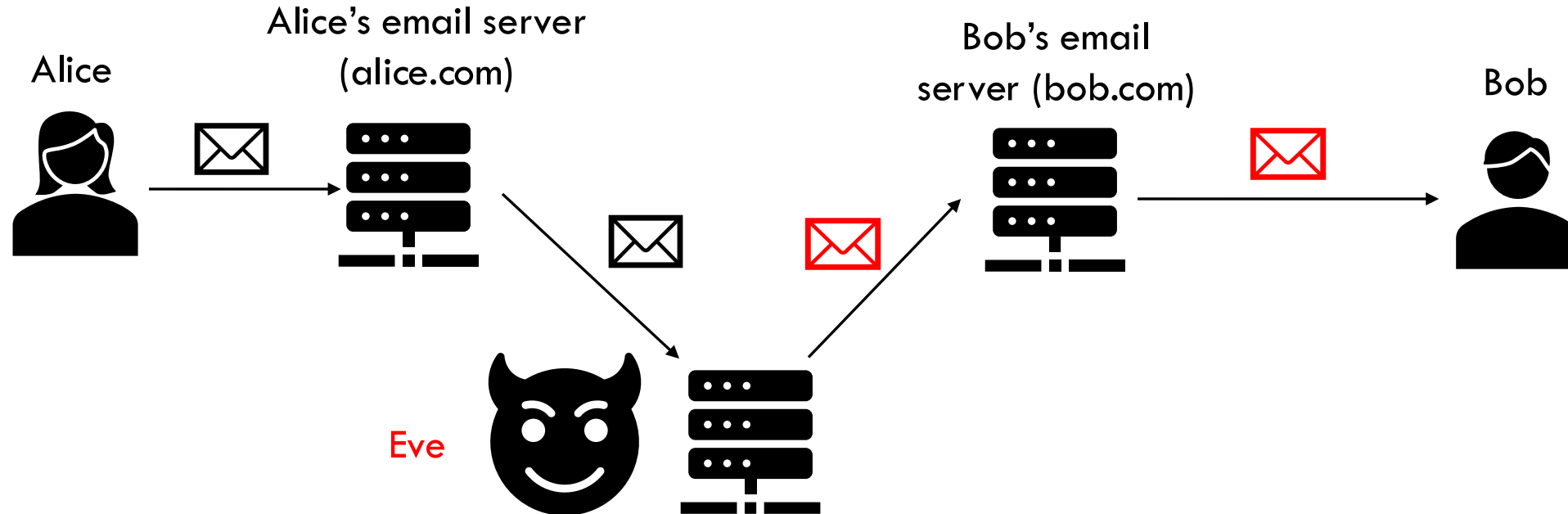
```
v=spf1 a -all
```

Alice's email server (alice.com)

- Allows current server (alice.com) send emails
- Unverified emails are not delivered
- Variants: add other servers, IP ranges...
- → A number of free SPF record generators available online

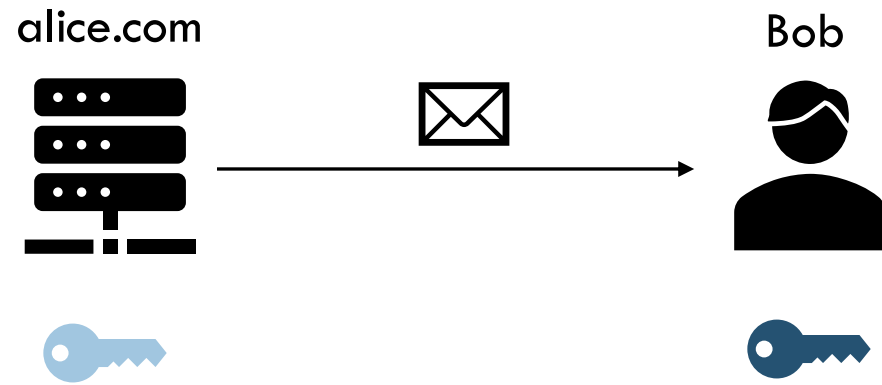


# DOMAIN VERIFICATION: MESSAGE SPOOFING



- Scenario: Eve wants to impersonate Alice
- She intercepts the message sent by Alice and changes its content before it gets delivered to Bob
- Solution: digital signatures via DomainKeysIdentified Mail (DKIM)

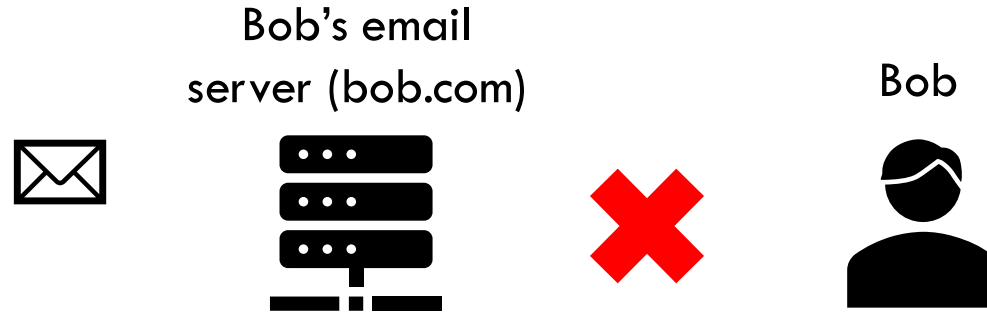
# DIGITAL SIGNATURE: HOW IT WORKS



- The *secret* key of alice.com needed to sign
- The *public* key of alice.com needed to verify the signature
- Signature ensures that
  - The email is sent via alice.com
  - It has not been tampered in transit



# DOMAIN VERIFICATION: DOMAINKEYSIDENTIFIED MAIL



“Has this message been signed with the public key of alice.com?”

No

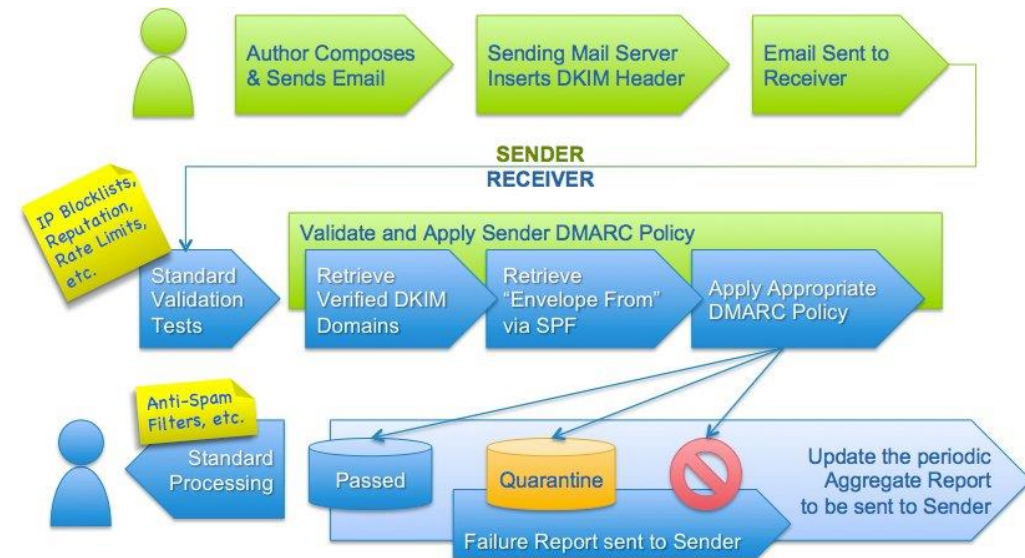
```
v=DKIM1;t=s;p=MIGfMA0GCSqGSIB3DQEBAQUAA4GNADCBiQKBgQDTQSnWt4zsHrr2ybQ1gq2L3Kbb035ZaPMKWHIRJ1NAyLIHctY8o/u05xMzYkX7opLTbpjJKI77C6z/pug8Z/NQntvx1Jam6++6WLuuzHgROBus+bJ23NFFhAnsEiEW75AhhwPEBWWDsmWqJ9rJs1Eh5FE5KKKVQ8hd88tOhpPzwIDAQAB
```

DNS records

The icon shows a server rack with three servers, representing DNS records.

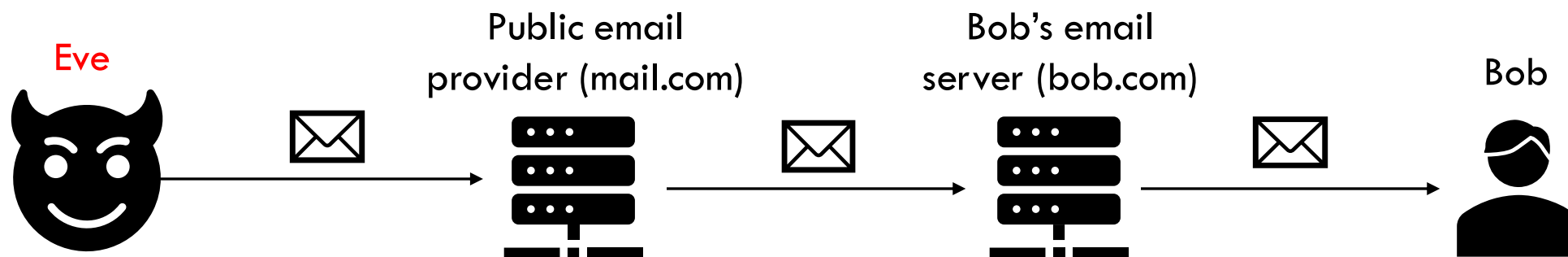
# DOMAIN VERIFICATION: DMARC

- Domain-based **M**essage **A**uthentication, **R**eporting and **C**onformance email standard
- Integrates records for SPF and DKIM
- Includes policies for how to handle emails based on check results, e.g. quarantine for further inspection or block
- Includes generating reports for senders
- **Currently recommended as a standard for email security** → see [dmarc.org](https://dmarc.org) for more information on implementation



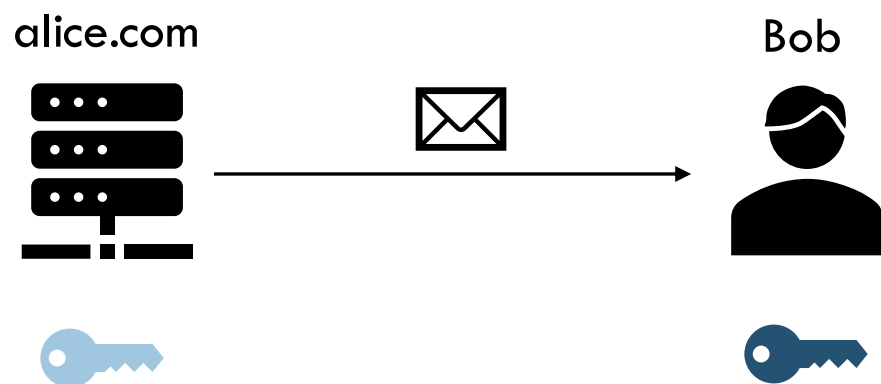
Source: [dmarc.org](https://dmarc.org)

# SENDER VERIFICATION



- Scenario: Eve wants to impersonate Alice
- She registers an account "alice-mail@mail.com" to use for sending her emails
- Domain verification would not work → all checks will pass!
- Solution: Alice's identity verification via digital signatures
- Difference to DKIM: Alice has her personal private and public key, not necessarily connected to specific email servers

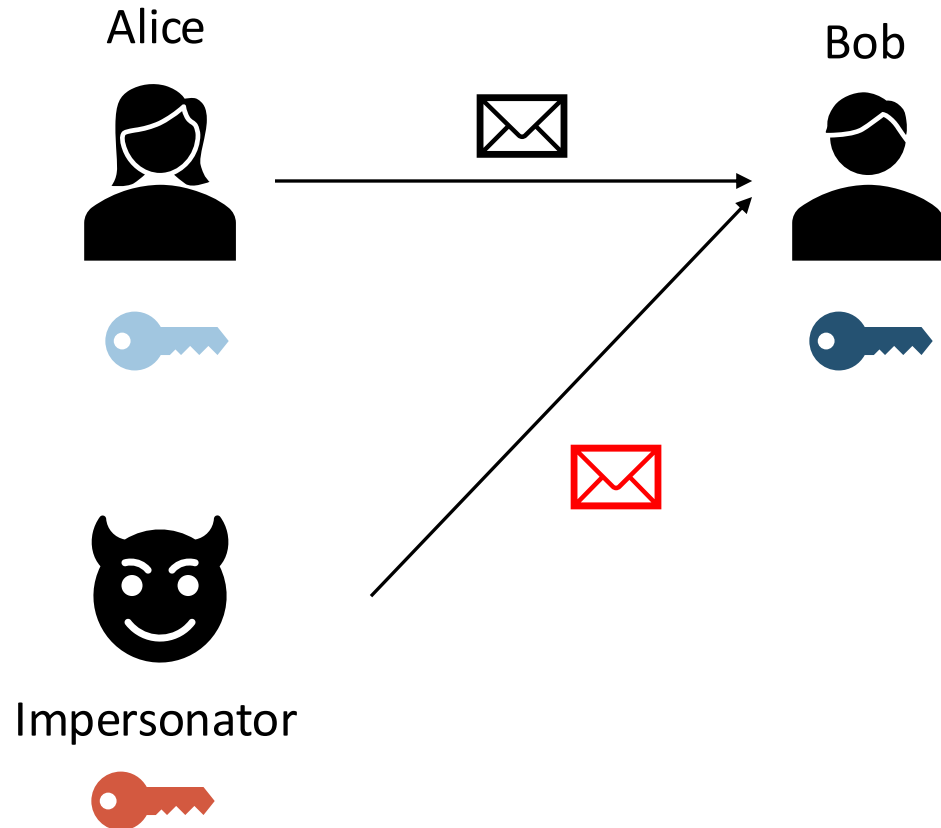
# DIGITAL SIGNATURE: SECURITY ASSUMPTIONS



- Alice's secret key needed to sign
- Alice's public key needed to verify the signature
- Signature ensures that the email is by Alice and has not been tampered in transit **under the assumptions:**
  - Only Alice has access to her secret key
  - The public key Bob uses for verification is actually from Alice



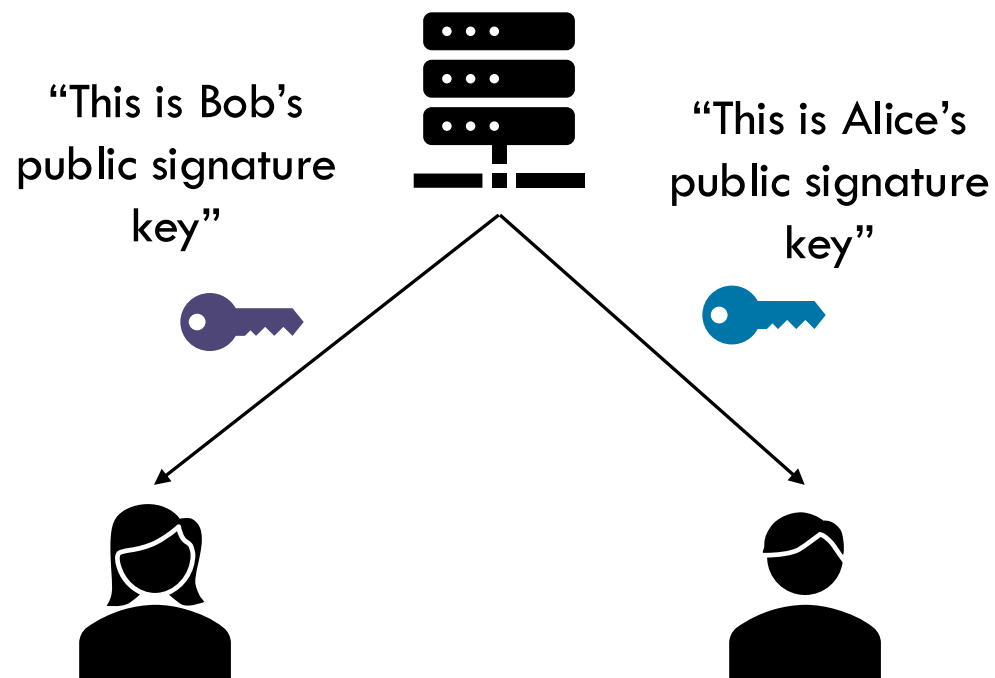
# DIGITAL SIGNATURE: PUBLIC-KEY INFRASTRUCTURE



- Main problem: key management
  - Eve uses her own private key to sign a message from "Alice"
  - Bob uses public key from Eve to verify the signature of "Alice"
- Assumption: existence of trusted PKI (Public-Key Infrastructure)



# DIGITAL SIGNATURE: CENTRALISED PKI



- Centralised: ownership of public keys confirmed by trusted authority
- Example: Secure/Multipurpose Internet Mail Extensions (S/MIME)
- Problem: only works if the authority is trusted by both Alice and Bob (e.g. internal company certification server)

→ Can be a problem with decentralised nature of email communication



# DIGITAL SIGNATURE: DECENTRALISED PKI



- Decentralised (“Web of trust”): Someone *whom Bob trusts* confirms that the public key he has comes from Alice
- Can be a trusted source such as Alice’s personal website, social media page...
- Example: Pretty Good Privacy (PGP)



# DIGITAL SIGNATURE: PROBLEMS

- Requires technical know-how to setup both for Alice to sign her messages and for Bob to verify them
- Key management becomes complicated
  - Finding correct public keys via decentralised PKI
  - Losing access to secret keys, e.g. due to data storage failure
  - Key revocation
  - Transfer of secret keys e.g. to multiple devices

→ Adoption rates of digital signatures in email is low

**MOTHERBOARD**  
TECH BY VICE

## Even the Inventor of PGP Doesn't Use PGP

Security is hard.

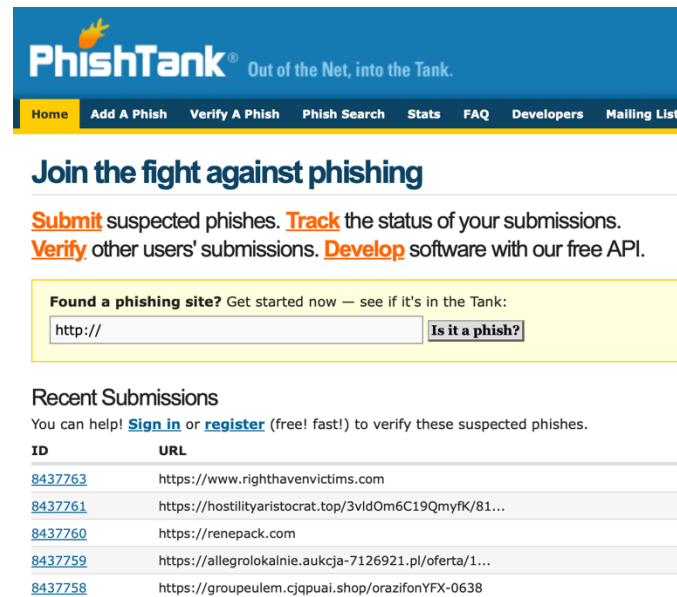
 By Lorenzo Franceschi-Bicchieri

Source: Vice



# BLOCKING OF MALICIOUS CONTENT

- Known malicious content
  - Known malicious domains (see e.g. PhishTank)
  - Known malware in attachments
- Potentially malicious content
  - Look-alike domains
  - Dangerous file formats in attachments (e.g. .exe)
  - Other suspicious indicators, e.g. certain keywords
- Alternative: only allow content from "allow-list", e.g. only internal websites → can be too restrictive
- Alternative: include a warning in a suspicious email instead of blocking it entirely → manual verification needed



The screenshot shows the PhishTank website. At the top, there is a blue header with the PhishTank logo and the tagline "Out of the Net, into the Tank." Below the header is a navigation menu with links for Home, Add A Phish, Verify A Phish, Phish Search, Stats, FAQ, Developers, and Mailing Lists. The main content area features a section titled "Join the fight against phishing" with instructions on how to submit, track, verify, and develop. Below this is a form for reporting a phishing site, with a text input field containing "http://" and a button labeled "Is it a phish?". Underneath the form is a section for "Recent Submissions" which includes a table of reported URLs and their IDs.

ID	URL
<a href="#">8437763</a>	<a href="https://www.righthavenvictims.com">https://www.righthavenvictims.com</a>
<a href="#">8437761</a>	<a href="https://hostilityaristocrat.top/3vldOm6C19QmyfK/81...">https://hostilityaristocrat.top/3vldOm6C19QmyfK/81...</a>
<a href="#">8437760</a>	<a href="https://renepack.com">https://renepack.com</a>
<a href="#">8437759</a>	<a href="https://allegrolokalnie.aukcja-7126921.pl/oferta/1...">https://allegrolokalnie.aukcja-7126921.pl/oferta/1...</a>
<a href="#">8437758</a>	<a href="https://groupeulem.cjqpuai.shop/orazifonYFX-0638">https://groupeulem.cjqpuai.shop/orazifonYFX-0638</a>



# AUTOMATIC VERIFICATION ISSUES

- Possible mistakes
    - False positives → legitimate emails are blocked
    - False negatives → phishing emails reach the user
  - Technical know-how required for certain methods, e.g. signing and verifying signatures
  - Threat intelligence can be lacking or outdated (e.g. in identifying malicious domains)
- Manual inspection sometimes needed



# MANUAL DETECTION INDICATORS

- Look and feel, e.g. spelling mistakes
  - Can be an indicator if the email is poorly made phishing email → might be enough to repel most of the attacks
  - However, professionally-looking phishing emails can be created
- Content of the email, e.g. suspicious requests, unusual wording, "Nigerian prince" frauds...
  - Can be an indicator in some cases (e.g. banks never asking for customers' credit card data)
  - However, hard to detect with personalised emails
- Lack of security features (domain verification/lack of signature)
  - Can be an indicator if such features are expected
  - However, false positives possible
  - False negatives not excluded (e.g. if DMARC set up incorrectly)
- URL/attachment check: most reliable indicator, but requires knowledge on behalf of the users



# PHISHING DETECTION METHODS: SUMMARY

- Block phishing websites? → not always reliable to detect or fast enough to act
- Register all alike domains → requires resources; what if the attacker comes up with new tactics?
- Protect against sender spoofing (e.g. DMARC) → might work, but what if the recipient doesn't know the valid sender address?
- Use digital signatures → might be too complicated for the users to apply
- Rely on users to detect phishing links → unavoidable, but **can be challenging**



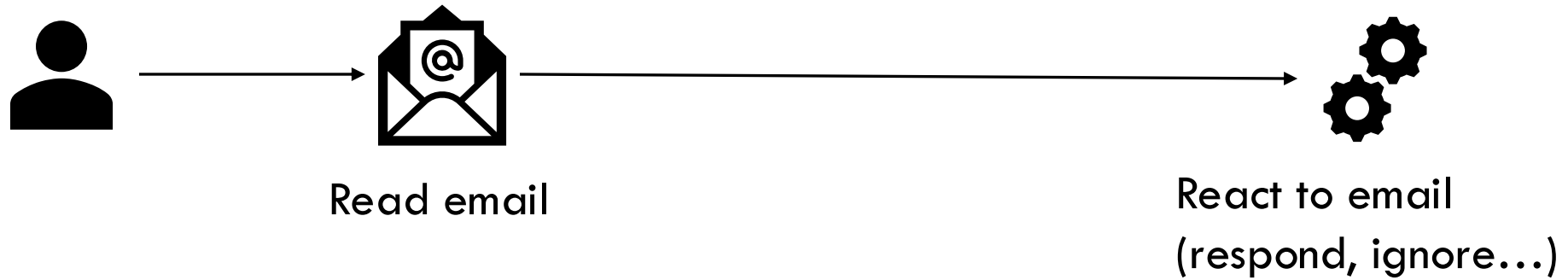


**Why teaching users to detect phishing is hard?**



# TASK: PROCESSING EMAILS

What the user wants to do



# TASK: PROCESSING EMAILS

What the user has to do



# WHY PHISHING WORKS

- Studies in 2006 and 2015
- Goal: investigate how people deal with phishing emails
- Reasons for failing to detect phishing
  - Lack of awareness (what phishing is)
  - Reliance on non-reliable indicators (website look & feel)
  - Misunderstanding of security indicators (HTTPS)
  - Bounded attention (security is a secondary task)

## Why Phishing Works

**Rachna Dhamija**  
rachna@deas.harvard.edu  
Harvard University

**J. D. Tygar**  
tygar@berkeley.edu  
UC Berkeley

**Marti Hearst**  
hearst@sims.berkeley.edu  
UC Berkeley

Why phishing still works: User strategies for combating phishing attacks ☆

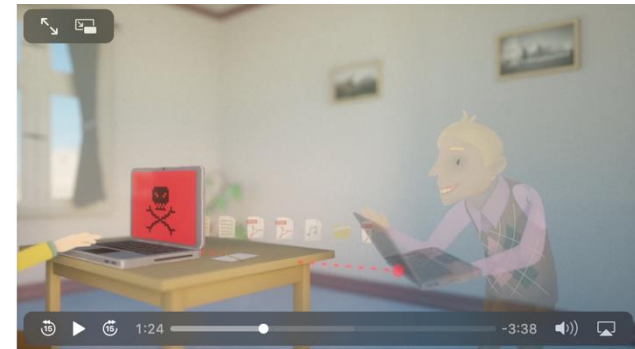
Mohamed Alsharnouby ✉, Furkan Alaca ✉, Sonia Chiasson 👤 ✉



# ANTI-PHISHING INFORMATION MATERIALS

- Variety of media available: e-learning modules, videos, websites, paper materials...
- Issues to consider
  - Passive learning
  - Need to motivate users to engage with the materials (brevity vs. completeness)
  - Quality of information needs to be ensured

Anti-Phishing materials from Karlsruhe institute of Technology:  
<https://secuso.aifb.kit.edu/english/1047.php>



Can you spot a fraudulent or suspicious email or text message?

Email and text fraud is becoming more sophisticated and effective, and more than half of all email is spam, according to 2018 data from Symantec.

#### Red flags to look out for:

- Subject line demands **urgent** or **immediate action**
- **Odd** or **unfamiliar senders**
- **Unexpected requests**

#### If you open the email:

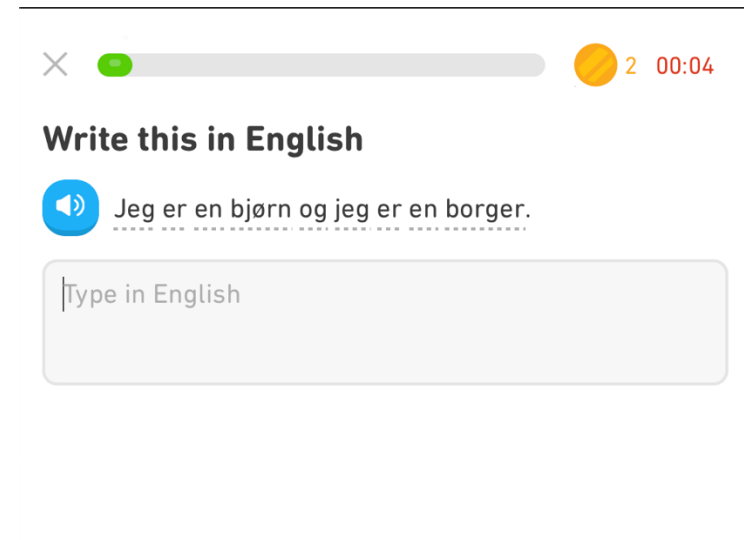
The body of a phishing or fraudulent email can be full of clues, but it can be difficult to distinguish from legitimate emails.

Anti-Phishing materials from Bank of America:  
<https://bettermoneyhabits.bankofamerica.com/en/privacy-security/how-to-avoid-email-scams>



# GAMIFICATION

- A common technique in education overall
  - Active learning
  - Motivation
  - Encourages regular repetition
- Application to security education: hacking challenges, CTFs, serious games...
- Potential disadvantages: simplification of contents, perceived to be "too childish"...

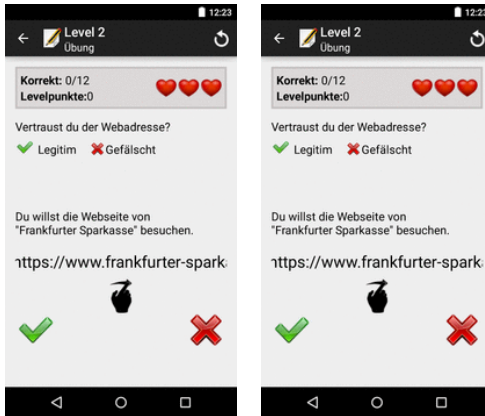


Source: Duolingo app

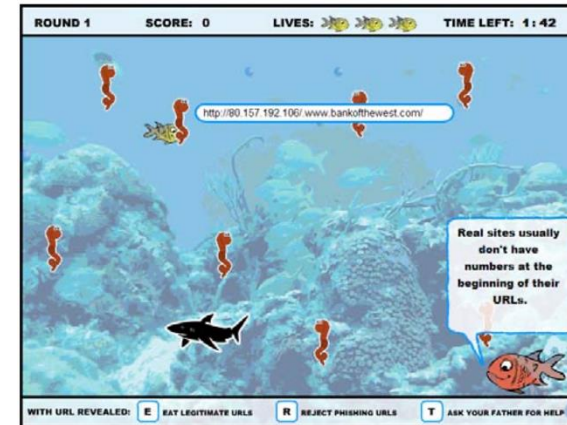


# ANTI-PHISHING GAMES

## Example: NoPhish



## Example: Anti-Phishing Phil



- Studies show promising results
- However, some issues remain
  - Some users unable to distinguish between phishing and legitimate links
  - Lack of integration in real-world context



# EMBEDDED LEARNING: CONCEPT

The graphic is a phishing education poster. At the top left is the APWG logo with the text 'Unifying the Global Response to Cybercrime'. At the top right is the Carnegie Mellon CyLab logo with the text 'Supporting Trust Decisions Project cups.cs.cmu.edu/trust'. In the center is a 'WARNING!' box with a penguin character pointing to it. Below the warning is a 'How to Help Protect Yourself' section with six numbered steps. To the left of the steps is a 'How You Were Tricked' section showing a woman looking at a computer screen displaying a phishing email and a browser address bar with a misspelled URL. To the right of the steps is a 'My Inbox' section showing a credit card statement and a phishing email attachment.

**APWG** Unifying the Global Response to Cybercrime

Carnegie Mellon **CyLab** Supporting Trust Decisions Project cups.cs.cmu.edu/trust

**WARNING!**

The web page you tried to visit might have been trying to steal your personal information. That page was removed after being identified as a "phishing" web page. A phishing web page tricks people out of bank account information, passwords and other confidential information.

**How You Were Tricked**

This email is from my bank. It asks me to update my information. I better click on the link and update it.

**STOP!**  
Don't fall for scam email.

**My Inbox**  
From: service@Wombank.com  
Dear Jane, Your account will be suspended if you do not update your information.  
<http://www.Wombank.com/update>

**How to Help Protect Yourself**

- 1 Don't trust links in an email.  
**DANGER!** <http://www.amazon.com/update>
- 2 Never give out personal information upon email request.  
**DANGER!** Name:   
Credit Card:
- 3 Look carefully at the web address.
- 4 Type in the real website address into a web browser.
- 5 Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.  
Credit Card Statement  
For Customer Service call: 1-800 xxx-xxx
- 6 Don't open unexpected email attachments or instant message download links.  
**My Inbox**  
Here is the updated document.  
[attachment](#)

- Idea: use *teachable moments*
  - Send simulated phishing emails
  - If recipient clicks on the link, forward them to the landing page
- Learning-by-doing in real-world context
- Can be seen as an industry standard

Source: <http://phish-education.apwg.org/r/index.html>

# EMBEDDED LEARNING: SUCCESS EVIDENCE

- A study with CMU students
  - 515 participants opting in
  - Retention study 28 days after the training
  - Three groups: control (no training), one-training and multiple-training
- Results
  - Decreased likelihood to click on phishing emails
  - Effects retain also after 28 days
  - More pronounced with multiple-training

## **School of Phish: A Real-World Evaluation of Anti-Phishing Training**

Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti,  
Lorrie Cranor, Jason Hong, Mary Ann Blair, Theodore Pham  
Carnegie Mellon University  
{pkumarag, jcransh, acquisti,  
lorrie, jasonhon, mc4t, telamon}@andrew.cmu.edu

→ **Problem solved?**





# EMBEDDED LEARNING: SUCCESS EVIDENCE

- Follow-up study
  - 1,359 employees
  - Participants informed about the real purpose *after* the study
  - Three phases of study with 3-4 months interval
- Two groups
  - Control (landing page with only a warning about being phished)
  - Training (landing page with additional information on how to detect phishing)



## Going Spear Phishing: Exploring Embedded Training and Awareness

Deanna D. Caputo | MITRE  
Shari Lawrence Pfleeger | ISIP Dartmouth College  
Jesse D. Freeman | MITRE  
M. Eric Johnson | Vanderbilt University



# EMBEDDED LEARNING: SUCCESS EVIDENCE

- Results: no significant improvement
  - No difference between training vs. no training
  - People who did not click on the link in the previous phases were less likely to click again
- Follow-up interviews: people admitting not to read the text on the landing page
- Reported feelings of fear, shame, anger (towards themselves and towards the study)...

→ Effectiveness of the training method inconclusive



## Going Spear Phishing: Exploring Embedded Training and Awareness

Deanna D. Caputo | MITRE  
Shari Lawrence Pfleeger | I3P Dartmouth College  
Jesse D. Freeman | MITRE  
M. Eric Johnson | Vanderbilt University



# EMBEDDED LEARNING: SUCCESS EVIDENCE

- Follow-up study
  - > 14,000 employees studied for over 15 months
  - Study integrated into company's awareness campaign
- Several conditions
  - Presence or absence of warning within the email
  - Embedded learning with training information on landing page vs. no information
  - Various types of report feedback

## Phishing in Organizations: Findings from a Large-Scale and Long-Term Study

Daniele Lain, Kari Kostiaainen, and Srdjan Čapkun  
Department of Computer Science  
ETH Zurich, Switzerland  
{daniele.lain, kari.kostiaainen, srdjan.capkun} @inf.ethz.ch



### Phishing

Identify dangerous e-mails quickly and reliably

You've just opened an Excel file named "Management levels 2019" and enabled the macros included in the document by clicking "Enable editing" and "Activate content" in the status bar. When you enabled editing, your computer could have been infected with malware (malicious software) in the worst-case scenario.



# EMBEDDED LEARNING: SUCCESS EVIDENCE

- Results: Embedded training does not improve future phishing detection rate
- Even worse: participants were more likely to click on a phishing link again after being exposed to a training page
- Possible explanations: sense of false security after seeing the landing page: "my company keeps me safe"

→ **Embedded learning can be harmful under certain conditions**

## Phishing in Organizations: Findings from a Large-Scale and Long-Term Study

Daniele Lain, Kari Kostiaainen, and Srdjan Čapkun  
*Department of Computer Science*  
*ETH Zurich, Switzerland*  
{daniele.lain, kari.kostiaainen, srdjan.capkun} @inf.ethz.ch



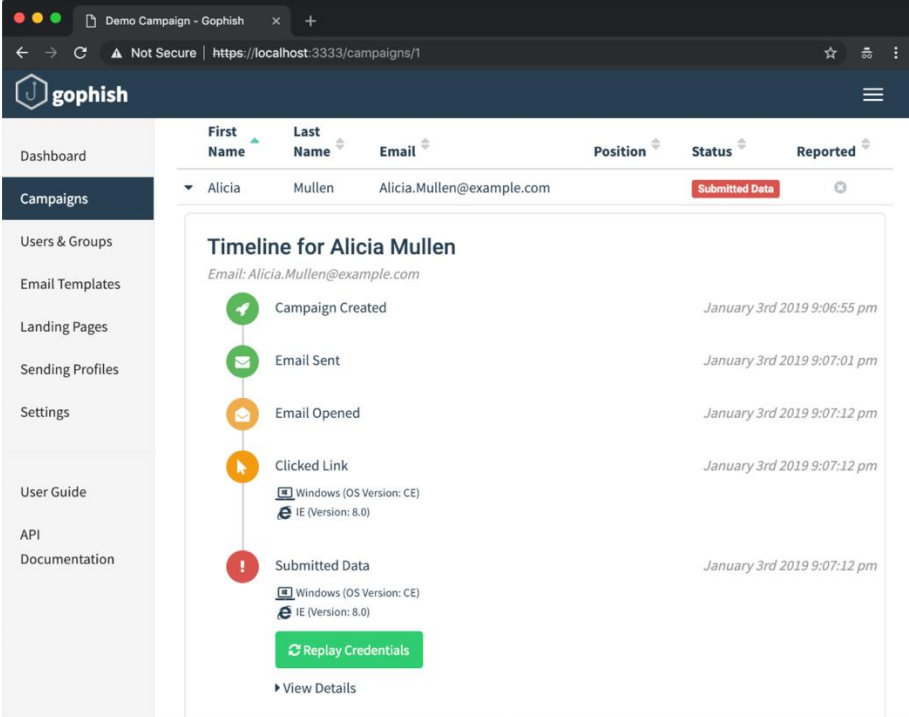
### Phishing

Identify dangerous e-mails quickly and reliably

You've just opened an Excel file named "Management levels 2019" and enabled the macros included in the document by clicking "Enable editing" and "Activate content" in the status bar. When you enabled editing, your computer could have been infected with malware (malicious software) in the worst-case scenario.

# SIMULATED PHISHING CAMPAIGNS

- Goals
  - Evaluation: how many people click on the link/enter their credentials?
    - How vulnerable the organisation is to phishing attacks?
    - How effective the conducted security awareness measures are?
  - Teaching, e.g. combined with additional awareness materials
- Collected data
  - Rate of clicks or data entries only
  - Names of people clicking or providing data (e.g. entering passwords) on the website
  - Specific data provided on the website



The screenshot shows the GoPhish web interface. The browser address bar indicates the URL is <https://localhost:3333/campaigns/1>. The dashboard header includes the GoPhish logo and navigation menus. A table lists campaign details for Alicia Mullen, with columns for First Name, Last Name, Email, Position, Status, and Reported. The status is 'Submitted Data'. Below the table, a 'Timeline for Alicia Mullen' is displayed, showing a sequence of events: Campaign Created (9:06:55 pm), Email Sent (9:07:01 pm), Email Opened (9:07:12 pm), Clicked Link (9:07:12 pm), and Submitted Data (9:07:12 pm). The Submitted Data event includes details for Windows (OS Version: CE) and IE (Version: 8.0). A 'Replay Credentials' button and a 'View Details' link are also visible.

Source: GoPhish platform blog



# SIMULATED PHISHING CAMPAIGNS

- Type of phishing emails: topics, difficulty in detection (e.g. spear phishing vs. more generalised phishing),...
- Time of distribution (e.g. one-off or prolonged campaign)
- Notification of employees in advance
  - Not notifying might lead to a more realistic scenario
  - However, ethical issues might arise
- Notification of employees during or after the campaign
  - Individual notifications e.g. after clicking on the link
  - Announcements at the end of the campaign

Security Architecture, Application security, Threat Management, Malware

f t e in

## 'Insensitive' phishing test stirs debate over ethics of security training

Bradley Barth September 29, 2020

**Justin Fenton**  
@justin\_fenton

After slashing our staff, closing newsrooms, furloughing reporters and cutting pay during a pandemic, @tribpub thought a neat lil way to test our susceptibility to phishing was to send a spoof email announcing large bonuses. Fire everyone involved.

We are pleased to inform you that we are providing targeted bonuses between 5,000 and 10,000 dollars this year. Tribune Publishing is able to provide this bonus as a direct result of the success created by the ongoing efforts to cut our costs!

We want to thank you for your ongoing commitment to excellence at Tribune Publishing, and to congratulate you on your outstanding performance!

You will need to login below to view your end of year bonuses. Please be advised that you may elect to deposit all or a portion of your bonus into the company RRSP program.

**KnowBe4**  
Human error. Conquered.

English - United States

Oops!  
You clicked on a simulated phishing test!

Remember these three rules to stay safe online:

- 01
- 02
- 03

# ISSUES WITH SIMULATED PHISHING CAMPAIGNS

- Weakening of email filters might be necessary, potentially leading to real phishing attacks coming through
- Attackers might use the campaign as pretext for their attacks
- If employees are informed (before or during the campaign), they might click on actual phishing links believing they are simulated ones (and therefore harmless)
- IT help desk might be overwhelmed with reports of simulated phishing emails and therefore miss the reports of real attacks

Other issues: legal, ethical... → see the study "Analysing Simulated Phishing Campaigns for Staff" by Volkamer, Sasse and Boehm



# ISSUES WITH SECURITY EDUCATION

- One-time measures are not enough
  - Habits take time to change
  - New people come to the organisations
  - Threats change, attackers become more clever etc.
- Putting responsibility solely on the user
  - Are there unreasonable demands on the users?
  - Do the users know how to report a phishing link?
  - Are there consequences for the user of reporting clicking on a phishing link?
- Lack of actionable advice
  - Instructions unclear ("don't click on suspicious emails")
  - Instructions unrealistic ("don't visit websites you don't know")



Source: <https://takefive-stopfraud.org.uk>




# FURTHER HELP IN DETECTING PHISHING


- Hints in email clients – warn if the link or the sender look suspicious
- Domain highlighting in browsers – help to identify the actual domain
- Password managers – if the website is not recognised, it might be a phish

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

Referred URL (also known as web address):  
<https://www.iconfinder.com>

TORPEDO classified this domain (highlighted part) as uncertain risk (grey frame). You have to assess the risk yourself in this case.

 **Please check the domain carefully.** Do not click the link unless you trust this domain. Otherwise, delete this e-mail.

 [More information on this classification](#)

TORPEDO has deactivated the link to give you time to check the domain carefully.  
Time remaining: 02 second(s).

Source: TORPEDO email plug-in  
(<https://secuso.aifb.kit.edu/english/TORPEDO.php>)



# PHISHING DETECTION ISSUES

- Limited attention span, only focusing on unusual emails
- Spear phishing attacks are hard to detect, especially if coming from a compromised account
- Effectiveness of tools hard to evaluate
  - Lab study – conditions different from real-world context
  - Simulated phishing campaigns – issues mentioned earlier



The background is a dark teal gradient. In the center, there is a faint, large circular graphic with a grid of dots. The corners of the page are decorated with white and light blue circuit-like patterns consisting of lines and circles. On the right side, there are several horizontal lines in shades of purple and pink.

## Measures against phishing: recommendations

# LAYERED APPROACH FOR ORGANISATIONS, NCSC

Make it harder for attackers to reach your users

Help users identify and report phishing emails

Minimise impact of phishing emails

Respond to incidents

→ See <https://www.ncsc.gov.uk/guidance/phishing> for more details



# MAKE IT HARDER FOR ATTACKERS TO REACH YOUR USERS

Make it harder for attackers to reach your users

Help users identify and report phishing emails

Minimise impact of phishing emails

Respond to incidents

- Prevent sending out emails from unauthorised senders
    - Blacklisting
    - DMARC
  - Consider information available to the attacker
    - Can the attacker learn names and emails of persons they might want to target and/or impersonate?
    - Can the attacker learn information about organisation (e.g. recent organisational changes) they can use to make their attacks more convincing?
- See "Social Engineering" lecture for methods of information gathering



# HELP USERS IDENTIFY AND REPORT PHISHING EMAILS

Make it harder for attackers to reach your users

Help users identify and report phishing emails

Minimise impact of phishing emails

Respond to incidents

- Use tools and education campaigns to inform users about features of phishing emails
  - Indicators such as sender, URL
  - Common tricks such as sense of urgency
  - Contextual indicators, e.g. does it make sense for this person to make this request?
- Provide reliable ways for users to get support or report phishing emails
  - Ensure communication channels to verify whether an email is legitimate
  - Ensure communication channels to report a suspicious email, including providing feedback
  - Avoid blaming the user



# MINIMISE IMPACT OF PHISHING

Make it harder for attackers to reach your users

Help users identify and report phishing emails

Minimise impact of phishing emails

Respond to incidents

- Goal: even if some users fall for phishing, the attacker should not be able to cause too much damage
- Regular updates and good security configuration – no malware infection just by visiting the website or reading the email
- Unique password for every account – leaked credentials will only give access to one account
- 2FA and other alternatives to passwords – stolen credentials are useless by themselves
- Least privilege – compromised accounts should not have too many rights



# RESPOND TO INCIDENTS

Make it harder for attackers to reach your users

Help users identify and report phishing emails

Minimise impact of phishing emails

Respond to incidents

- Goals of incident response
  - Timely reaction to ongoing attacks (e.g. by blocking specific senders or compromised accounts)
  - Threat intelligence for future attacks
- How to approach incident response
  - Provide reporting channels for users → security culture important for ensuring that users choose to report incidents
  - Set up monitoring tools for detecting unreported attacks (e.g. via security logging systems)
  - Plan incident response processes





# SUMMARY

- Phishing is a serious threat to organisations and end users
- Individual measures are helpful but not sufficient in isolation
  - Technical measures to block phishing emails, e.g. DMARC
  - Educating users how to recognise phishing
  - ..
- A holistic approach is required
  - Combination of prevention, detection, mitigation measures
  - Technical measures integrated with user education
  - Critical to ensure good security culture in an organisation



FIND OUT MORE

<https://gameSS.dk/>

GameSS 

# WHO IS BEHIND



## Partners behind the project



IT UNIVERSITY OF CPH



AALBORG UNIVERSITET



## Collaborators



## Supported by



Uddannelses- og  
Forskningsministeriet

Ministry of Higher  
Education and Science  
Denmark

