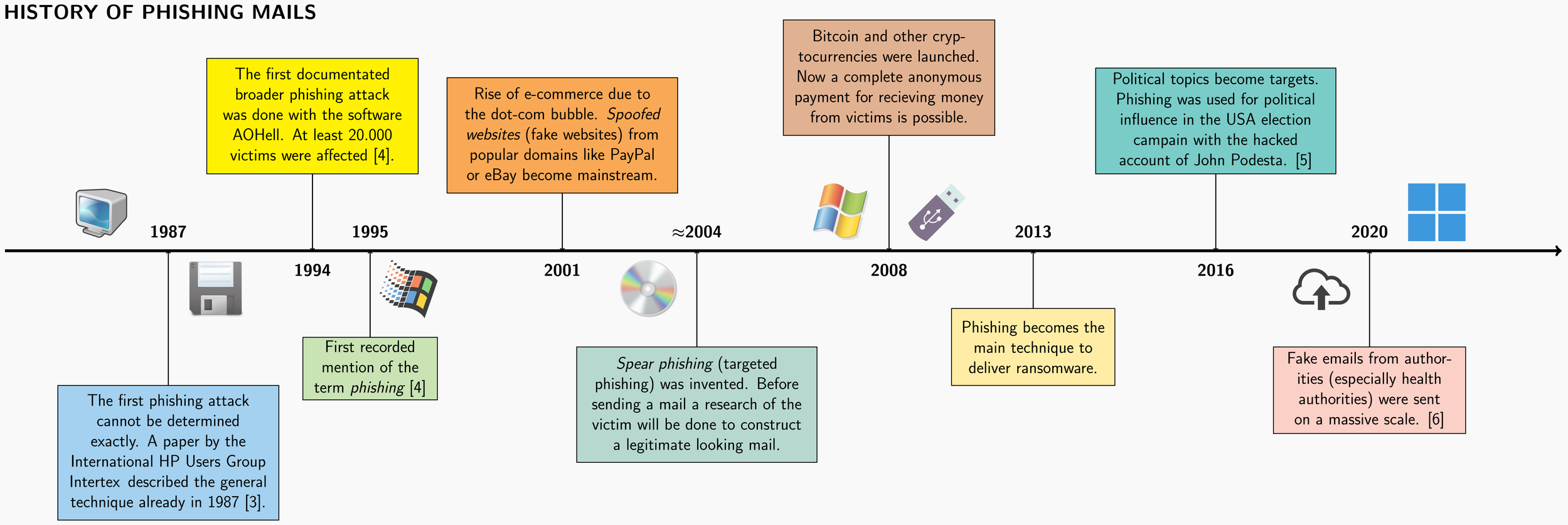
The evolution of Phishing mails

Introduction

An email is not a secure communication method. This is an advice given from global companies like Google and also from governments across the world.
The underlying technology was **designed in the 80s** [1]. Back in this time, there was no widely available encryption or authentication; so both of this security aspects were not considered much.

The lack of authentication makes it possible, that everyone can send fraud emails that appear to be from a trusted source, such as a government agency or a bank. Such an attack is called phishing. This is, as of 2020, most common type of cybercrime [2]. This poster summarizes the evolution of phishing mails back from the beginning to today and provides information on how to recognize phishing mails and whether the situation will improve in the future

HISTORY OF PHISHING MAILS



Examples of real phishing mails

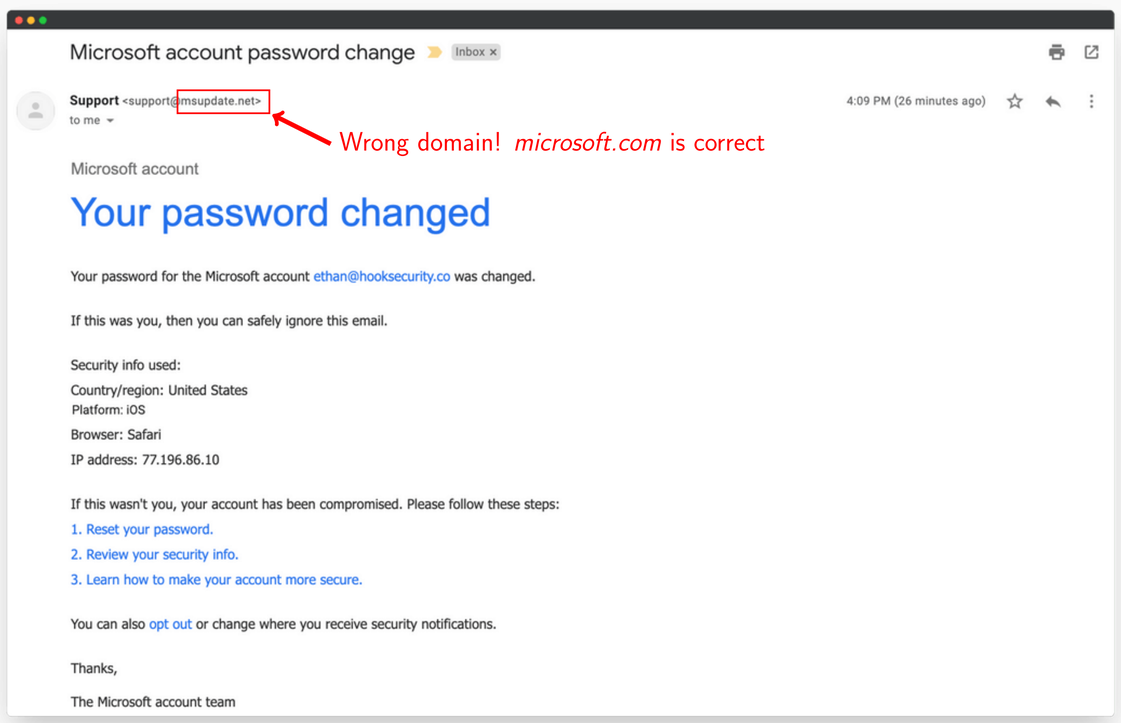


Figure: Microsoft phishing mail ≈2018 [7].

```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* xxxxxxx@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
> xxxxxxx@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.
```

Wrong domain! *google.com* is correct

Shortend link!

Figure: The John Podesta email released by WikiLeaks in 2016 [5].

Tipps to identify phishing mails

- Subtle misspellings in the sender's address
  - "g**00**gle.com" instead of "g**oo**gle.com"
  - "microsof**f**.com" instead of "microsof**t**.com"
- Unfamiliar greetings or missing name in the greeting ("Hi", "Hello", "Dear customer")
- Grammar and spelling mistakes
- Creating time pressure
  - "Your account will be suspended in the next few days"
  - "Action required"
- Requesting for personal information
- Unusual file types in the attachment (e.g. ".exe", ".bat", ".java")

Conclusion

If email were developed today, the technical design would be completely different. Nevertheless, despite its technical problems, email will not lose its importance. Because although we are now more networked than ever, we are also more fragmented than ever. Sending a message from one messenger service to another is not possible. The same applies to the countless social media platforms. Email is the only generally accepted technology that works across platforms. *This technology is not good, but it's the best we have.*

If current trends continue, the number of phishing mails will continue to increase. And recognizing them will also become increasingly difficult. Not least due to the constant development of large language models.

The problem with phishing mails cannot be solved technically in practice. The only possibility that exists is education!

REFERENCES

1. https://datatracker.ietf.org/doc/html/rfc821
2. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
3. Felix, Jerry & Hauck, Chris (September 1987). "System Security: A Hacker's Perspective". 1987 Interex Proceedings. 8: 6.
4. https://web.archive.org/web/20051214053144/http://wired-vig.wired.com/news/technology/0%2C1282%2C9932%2C00.html
5. https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/
6. https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Warnhinweise/200507_Coronaphishing.html
7. https://www.hooksecurity.co/phishing-examples/microsoft-phishing-example

Created with LaTeX
Get the PDF and the source code via this QR code.