IT STARTED WITH A PHISH...



We all think we're too smart to believe our long lost zillionaire uncle in Timbuktu left us a fortune. But most cybercriminals are too smart to think you'll fall for it – and have adjusted their techniques to make them much more believable. Which is why more people than ever are clicking...and businesses are struggling to stop phishing attacks making it to the end user.

Born in hell

The first known mention of "phishing" was in a Usenet group called 'AOHell' on January 2nd 1996. Ironically, AOHell was an app used to steal passwords and credit card details from AOL users.

Share the love

In 2000, the **'Love bug' a phishing attack** prompting users to open an attached 'love letter' hit **45 million users**. The virus sent itself to everyone in the victim's address book.

Click, click, BOOM!

1/2 people will click on an unsolicited mail, despite **78%** saying they understand the risks.

1/2

Big business

Increase in business email compromise scams, with over **$3bn** in losses since 2015.

+ 1,300%

Asking for trouble?

Percentage of business IP sent via email.

80%

Capital flight

$54m = the amount of money stolen in a business email compromise attack on from Austrian aeroplane parts maker FACC AG in 2016.

Landing the big catch

Number of people **who fall for a phishing scam** every day.

80,000

Spot the difference?

Cyber criminals are creating an average of around **1.4 million phishing websites every month** with fake pages designed to mimic the company they're spoofing

Fraudster's favorites

Facebook, Microsoft and Yahoo! are the **top 3 most faked brands** used in phishing attacks.

It started with a phish

80% of data breaches involve stolen or weak passwords, most of them acquired via phishing emails[3]

Show them the money

More than half of all phishing attacks target the financial sector: 26% attack banks, **13%** payment systems and **11%** online shops.

Most targeted country

20%	Brazil
16.5%	Australia
15.6%	New Zealand

59,569,508

Number of **attempted visits to phishing pages blocked** by Kaspersky Lab in Q3 2017

Smish and grab

Mobile phone-based phishing is called 'smishing'. Smish attacks are usually banking-related.

Attack of the clones

Clone phishers replace legitimate, previously delivered content with malicious mails and attachments – the technique is usually of the "Whoops, I sent the wrong info, use this one" variety.

Be prepared

2017's bumper year for phishing-related data theft is widely predicted to become 2018's mass spear-phishing problem, as data stolen in 2017 will be used to launch highly tailored attacks. It only takes one dodgy mail to bring down your business. Don't get hooked – try Kaspersky Security for Microsoft Office 365 today and block phishing and other email threats before they become a problem.

[1] http://www.phishing.org/history-of-phishing / [2] Friedrich-Alexander Universitat: https://www.fau.eu/2016/08/25/news/research/one-in-two-us-ers-click-on-links-from-unknown-senders/ / [3] FBI's Internet Crime Complaint Center (IC3) / [4] https://www.pcmag.com/feature/357913/securi-ty-in-2018-buckle-up-this-isn-t-getting-any-easier/2 / [5] http://www.securityweek.com/cybercriminals-steal-54-million-aircraft-parts-maker / [6] Canadian Department of Public Safety & Emergency Preparedness / [7] http://www.zdnet.com/article/1-4-million-phishing-web-sites-are-created-every-month-heres-who-the-scammers-are-pretending-to-be [3] Verizon Data Breach Investigation Report 2017. / [8] https://www.kasper-sky.com/about/press-releases/2017_5000-fold-decrease-in-spam-botnet-mailings / [9] https://securelist.com/spam-and-phishing-in-q3-2017/82901/

KASPERSKY lab