

THE HISTORY OF PHISHING



Phishing scams are a common tactic that cyber criminals use to steal your personal and financial information. Cyber criminals have been using this scheme since the word **internet** was defined in the 1990s, and their methods have become increasingly sophisticated over time.

Here's a brief history of how phishing campaigns have evolved into what they are today:

1990s



Though it may have existed before this, the first phishing attempt is recorded on **America Online Inc. (AOL)**. Hackers attempt to steal login credentials and personal information from AOL users to resell them online.



6.4 billion
phishing emails
are sent worldwide
every dayⁱ



1996

The term "phishing" is created by a group called AOHell.



2000s

2001 •

The rise of e-commerce encourages cyber criminals to create **spoofed websites**, impersonating popular domains like eBay and PayPal.

2004 •

Hackers start using pop-up windows to gather sensitive information from unsuspecting users. Techniques like **spear phishing**, smishing and keylogging are created.

2008 •

Bitcoin and cryptocurrencies are launched. This increases the creation of malware as it is easier for cyber criminals to securely (and anonymously) receive payment from their victims.

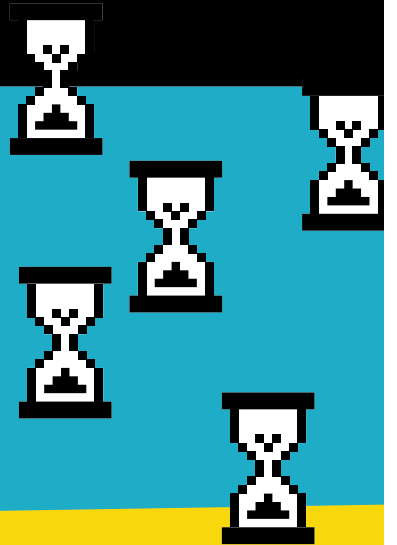
FACT

**Approximately
\$929 million
in losses were caused
by phishing between
2004-2005.ⁱⁱ**

2010s

2013 •

Phishing becomes the primary technique to deliver ransomware.



2017

Hackers adopt HTTPS on their spoofed sites.

2018 •

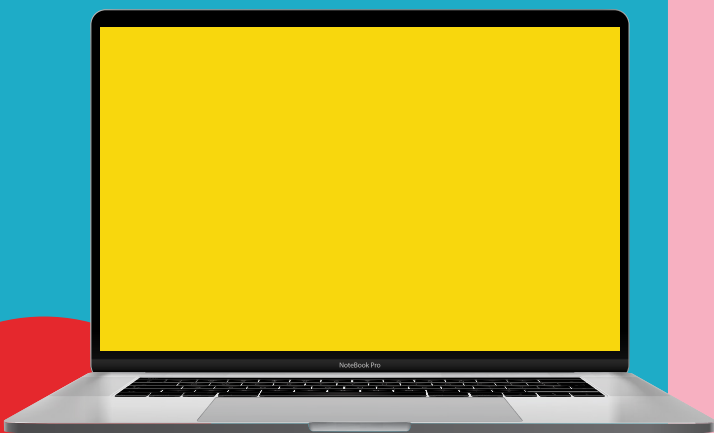
Cyber criminals begin hiding malicious code inside image files to slip through a user's anti-virus software.

2019

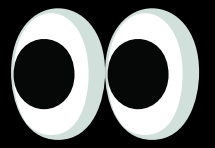
Gift card phishing campaigns become more complex, offering victims incentives and bribes. Phishing attempts also start to threaten victims with legal action or incarceration if gift cards or bitcoin aren't sent to cyber criminals.

FACT

In 2018,
85% of Canadians
said they received a
phishing email.ⁱⁱⁱ



2020s



Phishing emails and calls run rampant with hyper-targeted campaigns launched at the public. Topics include COVID-19 and the Canadian Emergency Response Benefit (CERB). Cyber criminals also target different user accounts such as those for popular streaming services and social media.

3 OUT OF 10

Canadian organizations saw a spike in the number of cyber attacks they received during the pandemic.^{iv}

Phishing campaigns can be tough to identify – especially when cyber criminals have become experts at tricking their victims into giving up their information.

YOU CAN AVOID BECOMING A VICTIM OF A PHISHING SCAM BY USING THE FOLLOWING TIPS:



Take a minute to think before you take action



Don't click strange links or open suspicious attachments



Check the email address for strange spelling or characters



Look for spelling or grammar mistakes



Watch out for poor formatting



Reach out to the sender through a different channel if you're not sure whether the message is real

GET MORE TIPS TO SECURE YOUR ACCOUNTS AND DEVICES AT

 [GETCYBERSAFE.CA](https://getcybersafe.ca)



Communications
Security Establishment

Centre de la sécurité
des télécommunications

Canada 

i. Valimail, 2018 Email Fraud Landscape, 2018

ii. History of Phishing, KnowBe4, 2021

iii. Canadian Cybersecurity Survey – Spring Edition, Canadian Internet Registration Authority (CIRA), 2018

iv. CIRA Cybersecurity Report, Canadian Internet Registration Authority (CIRA), 2020