

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 scams are a common tactic that cyber criminals use to steal

into what they are today:

phishing campaigns have evolved

## Though it may have existed before this,



America Online Inc. (AOL). Hackers attempt to steal login credentials and personal information from AOL users to resell them online.

the first phishing attempt is recorded on

billion



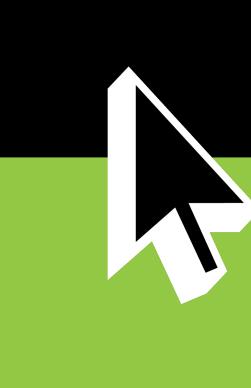
The term "phishing" is created by a group called AOHell.



spoofed websites, impersonating popular domains like eBay and PayPal.

The rise of e-commerce encourages

cyber criminals to create





unsuspecting users. Techniques like spear phishing, smishing and keylogging are created.

2004

Hackers start using pop-up windows

to gather sensitive information from

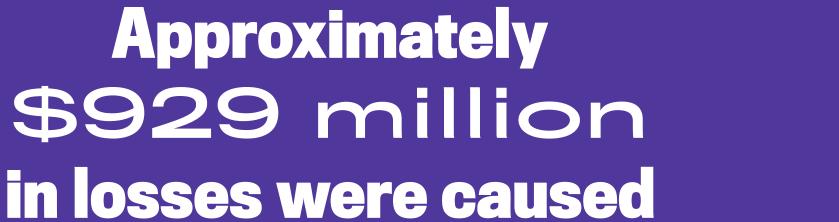
payment from their victims.

launched. This increases the creation of

malware as it is easier for cyber criminals

to securely (and anonymously) receive

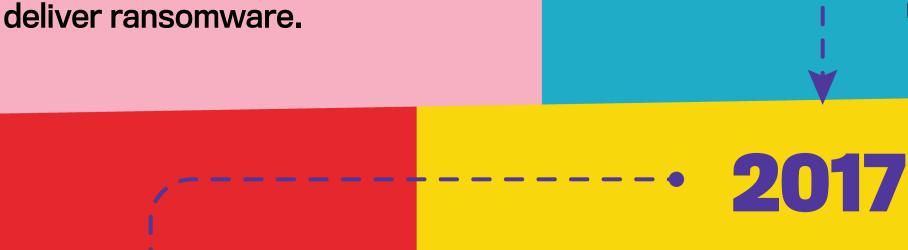
FACT



2013 ·---

by phishing between

2004-2005.<sup>ii</sup>



• 2017

Hackers adopt HTTPS on their spoofed sites.



Phishing becomes the

primary technique to

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.





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.

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

have become experts at tricking their victims

into giving up their information.

FACT

## Phishing campaigns can be tough to identify – especially when cyber criminals

3 OUT OF 10

Take a minute to think before you take action

AVOID
BECOMING

A VICTIM OF

Take a minute to think before you take action

Don't click strange links or open suspicious attachments

Check the email address for

Ŧ

Reach out to the sender through a different channel if you're not

Look for spelling or

grammar mistakes

sure whether the message is real

strange spelling or characters

Watch out for poor formatting

GET MORE TIPS TO SECURE YOUR ACCOUNTS AND DEVICES AT

GETC BERSAFE.CA

Communications Centre de la sécurité
Security Establishment des télécommunications

**A PHISHING** 

USING THE

FOLLOWING

SCAM

TIPS:

Canada

Catalogue number: D96-69/2021E-PDF | ISBN: 978-0-660-39741-2