## Think Before You Click



describe how bad actors manipulate individuals into giving them access to personal information. Phishing is the most common form of social engineering for stealing an individual's personal information like IDs or passwords, or for installing malware which can be used for various purposes including ransomware attacks.

Social engineering is a general term used to

300% Rise in ransomware attacks in

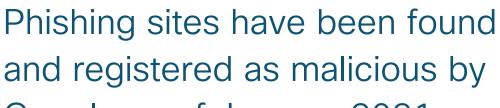
the US in the past year.1

94% Of malware on computers found

their way there via phishing email.<sup>2</sup>

67.5% Of individuals that click on a phishing

link are likely to enter their credentials on a phishing website.3



2 Million+

Google as of January 2021.





### Phishing attacks are easier to avoid when you know how to spot them It only takes one wrong move for cybercriminals to access your data

organization by learning how to recognize common phishing tactics. **Email Phishing** 

or your company's systems. Protect yourself, your family, and your

## 96% of all phishing attacks come via email.4

An email sent with the intention of

deceiving you to act, such as updating a

password or clicking on an attachment.

**Smishing** Phishing via text. The fraudulent text may appear to come from a reputable business, but is designed to trick you into revealing personal information.



### immediately.

**Vishing** 

**Angler Phishing** Targets social media users. Bad actors will direct message disgruntled customers, pretending to be customer service agents, to obtain personal information or other

Also known as voice phishing occurs via

believe they will be fined or miss out on a

phone. The caller typically leaves an

"urgent" message, making recipients

potential windfall if they don't respond

### otherwise legitimate websites that have been infected with malicious code and entice you to click on them to corrupt

your device or data.

Pop-up Phishing

account credentials.

Verify before you act

Never give out personal or

When receiving email from

known institutions (government,

banks, your doctor), go directly

to the source instead of clicking

an email request.

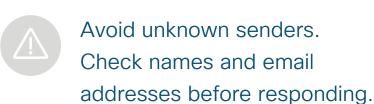
on links in the email.

phishing.

financial information based on

Fraudulent messages that "pop up" on

# can steal sensitive information or redirect links to malicious sites. Don't take the bait.



Avoid unknown senders. Check names and email

in unsolicited emails.



Be suspicious of emails marked "urgent."

Beware of messages with

Don't trust links or attachments



Don't be lured by "deals". They are usually too good to be true.

mistakes in spelling or grammar.



Consider finding an email provider that is more secure than the free options.



Be wary of generic greetings, such as dear sir or ma'am. Understand your service provider's

policy for tracking and stopping



help access to your computer.

Don't give a stranger or unsolicited

It's time to rethink email security Cisco Secure Email rapidly detects, quarantines, investigates, and remediates

platform, included with each email license, provides enhanced visibility, automation,

### and a layered approach to security across all of our Cisco Secure products. Learn more

phishing and other cyberattacks that target your email. Plus, our built-in SecureX

Click here for more information about the

**Anatomy of a Modern Phishing Attack** 

© 2021 Cisco and/or its affiliates. All rights reserved.