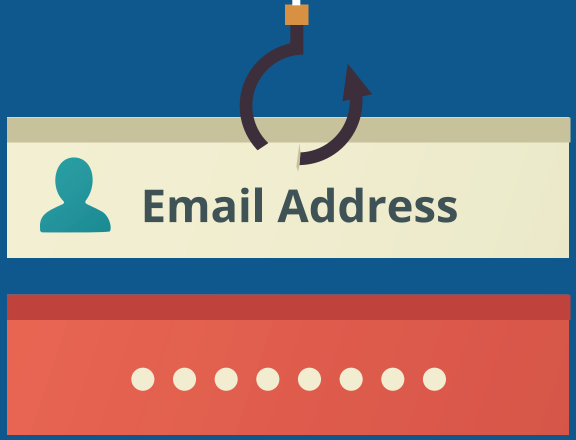
A COMPLETE GUIDE TO PHISHING SCAMS:

The Facts, Pitfalls & Solutions You Need to Know



PHISHING FACTS: WHAT YOU DON’T KNOW CAN HURT YOU

Modern cyberattacks are not only increasing in number, but they are also more complex. Today’s cybercriminals are smarter and continually inventing new techniques to get what they want. And while email scams aren’t anything new, they are becoming increasingly more sophisticated. They lure you in with their big brand names and scare tactics. And the repercussions of falling victim can be insurmountable.

$3.86 MILLION

Average cost of a data breach

Source: IBM

#1

Phishing is the most common type of cybercrime

Source: FBI

39 SECONDS

Hackers attack every 39 seconds

Source: University of Maryland

43%

Of cyberattacks target small businesses

Source: Accenture

60%

Of small businesses fold within six months of a cyberattack

Source: Inc.

95%

Of cybersecurity breaches are caused by human error

Source: IBM

PHISHING WORKS BECAUSE IT’S CONVINCING

Here are some of the most common types of phishing scams. The common thread is to lure you in so that you take the bait.

Phishing

scams use social engineering techniques, like email, to trick a person into providing sensitive information.

Spoofing

is when criminals disguise themselves as trusted sources, either as an individual or an organization.

Spear phishing

targets a specific individual in an attempt to gain sensitive information.

Whaling

otherwise known as CEO fraud, occurs when cybercriminals impersonate a CEO or other high-ranking executive.

Vishing

scams occur when criminals trick people into giving up confidential information through deceptive phone calls.

Search engine phishing

involves cybercriminals working to get their malicious website included in a legitimate list of search results.

Smishing

scams are phishing scams deployed via text (or SMS) messages.

Malvertising

happens when cybercriminals embed malicious code into legitimate-looking advertisements.

What’s Your Data Worth?

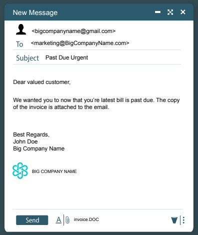
Data breaches can be damaging enough when you consider the potential financial and legal implications. But consider where your private information could end up. Account login credentials, credit card numbers, Social Security numbers, home addresses, dates of birth and more could all potentially turn up for sale on the dark web.

A PHISHING PATH TO THE DARK WEB

START

1\.

You get an email from a national vendor notifying you about a past due bill.



New Message

<bigcompanyname@gmail.com>

To <marketing@BigCompanyName.com>

Subject Past Due Urgent

Dear valued customer,

We wanted you to now that you're latest bill is past due. The copy of the invoice is attached to the email.

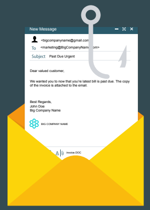
Best Regards,
John Doe
Big Company Name

BIG COMPANY NAME

Send invoice.DOC

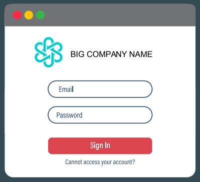
2\.

You recognize the email because you receive emails from this vendor regularly.



3\.

It looks right, so you click on the link provided.



BIG COMPANY NAME

Email

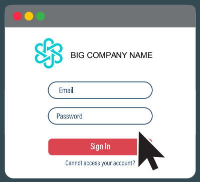
Password

Sign In

Cannot access your account?

4\.

The link redirects you to a fraudulent site spoofed to replicate the vendor's login page.



BIG COMPANY NAME

Email

Password

Sign In

Cannot access your account?

5\.

It looks legitimate, so you log in with your username and password.

END

6\.

Now the cybercriminals have access to your account and any information stored there.

WHAT IS THE DARK WEB?

The dark web is comprised of webpages hidden just underneath the webpages you browse daily on the surface.

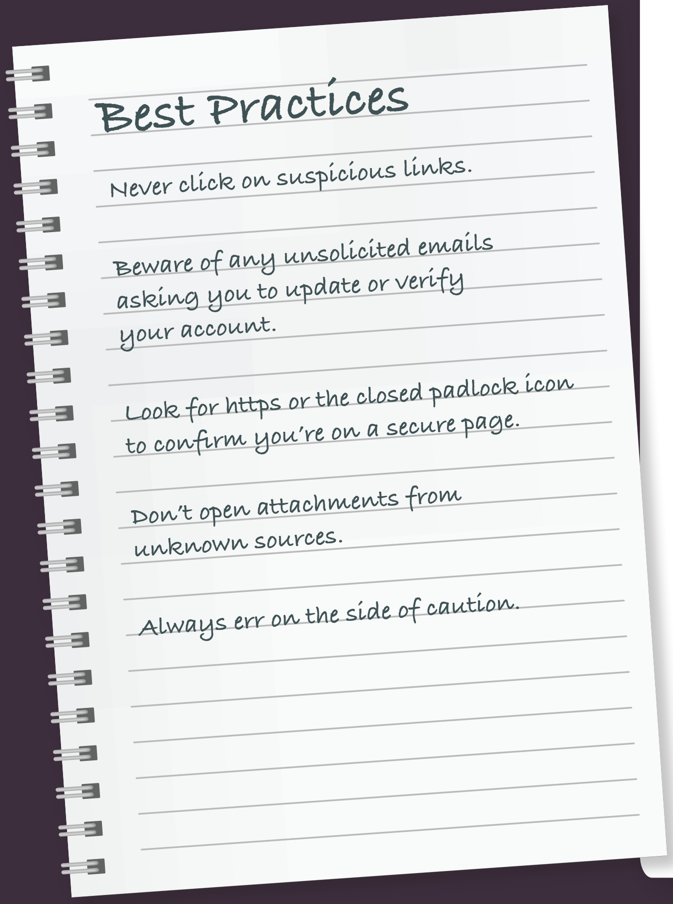
You can search the dark web anonymously by downloading a dark web browser and using a VPN. Understandably, the inherent anonymity of the dark web attracts questionable characters and shady deals. Most transactions are conducted using cryptocurrency.

What's at Stake?

A successful phishing attack can result in:

- **Financial loss**
- **Exposed customer and employee information**
- **Compromised accounts**
- **Ransomware infections**
- **Lost intellectual property**
- **Locked, inaccessible documents**
- **Damage to employer reputation**
- **Legal fees and compliance fines**

CAN YOU RECOGNIZE A PHISHING SCAM?



Best Practices

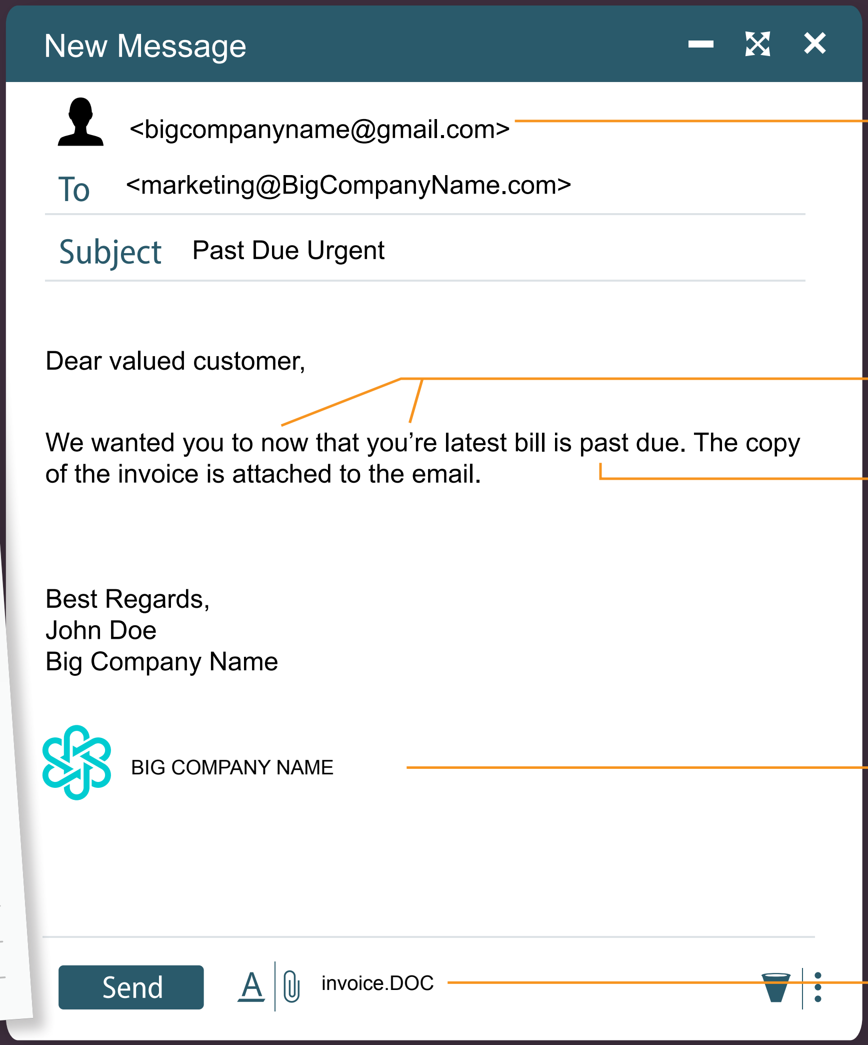
Never click on suspicious links.

Beware of any unsolicited emails asking you to update or verify your account.

Look for https or the closed padlock icon to confirm you're on a secure page.

Don't open attachments from unknown sources.

Always err on the side of caution.



<bigcompanyname@gmail.com>

To <marketing@BigCompanyName.com>

Subject Past Due Urgent

Dear valued customer,

We wanted you to now that you're latest bill is past due. The copy of the invoice is attached to the email.

Best Regards,
John Doe
Big Company Name

BIG COMPANY NAME

Look closely at the sender name and the URL.

Look for bad grammar and misspellings.

Be suspicious of emails with urgent, time-sensitive messaging.

Common reputable companies imitated: Google, Dropbox, YouTube, Facebook, Amazon and Apple.

Common types of malicious files attached: Windows executables, script files, Office documents

THE BEST DEFENSE IS A MULTI-PRONGED DEFENSE

Cybersecurity Training

Keep employees up to date and mindful of potential threats with ongoing security awareness.

Backup and Recovery

Maintain frequent backups in multiple locations and test often.

Multi-Factor Authentication

Stop unauthorized user access to your data by requiring multiple methods of identification.

Computer Updates

Automate software updates and security patches to protect your computers from the latest attacks.

Email Security Filters

Prevent suspicious emails from hitting your inbox with the right anti-spam software.

Mobile Device Protection

Protect your employees' devices from hackers attempting to steal your data or access your network.

CONCLUSION

Successfully defending your business against cyberthreats is an ongoing, multi-faceted effort.

When you’re looking for a partner in the fight against cybercrime, contact us. Our staff is well-versed in proven, innovative techniques that deter cyberbreaches and avoid data loss.

Is Your Business at Risk?

Contact us, and learn the benefits of a security assessment.