101domain.com Corporate Brand Services

The Enterprise Guide to Cyber Attack Prevention

You've built your business and your brand. Now how do you secure and protect it?

Cyber Attacks

Cyber Attacks

CONTENTS

INTRODUCTION

When we hear about companies who suffer from data breaches and digital heists, we usually imagine massive cyber attacks as the culprit behind them.

However, attacks do not always require forceful entry to your code or webservers. In fact, in most cases, all the attacker has to do is ask nicely. We are talking about email spoofing attacks directed at vulnerable employees in your accounting and finance departments. This sophisticated threat, known as spear phishing, is difficult to defend against because it plays on human emotion and requires intuitive decision-making.

Imagine what would happen if one of your employees was tricked into transferring funds or sharing sensitive information with an outside individual impersonating someone in another department of your organization, or bearing the brand of your trusted third-party partner? A simple mistake could cost your company millions of dollars.

In this whitepaper, we will cover different types of cyber attacks, including how to spot the warning signs of a spear phishing attack or other email spoofing attacks. Most importantly, we will share the tools you can use to educate your employees, monitor your brand name, and detect malicious activities before they cause irreversible damage.

CYBER ATTACKS TARGET ALL BUSINESSES

YES, SMALL BUSINESSES TOO

> ***My company is so small it wouldn't be worth it for someone to go after us.***

This is a common misconception. In reality, small businesses are low-hanging fruit because they don't think that they are a target.

According to a report by technology consulting firm Kelser Corporation, 43% of cyber attacks target small business. In addition, 1 out of 5 businesses will fall victim to an attack simply because they aren't prepared for one.

TYPES OF CYBER ATTACKS

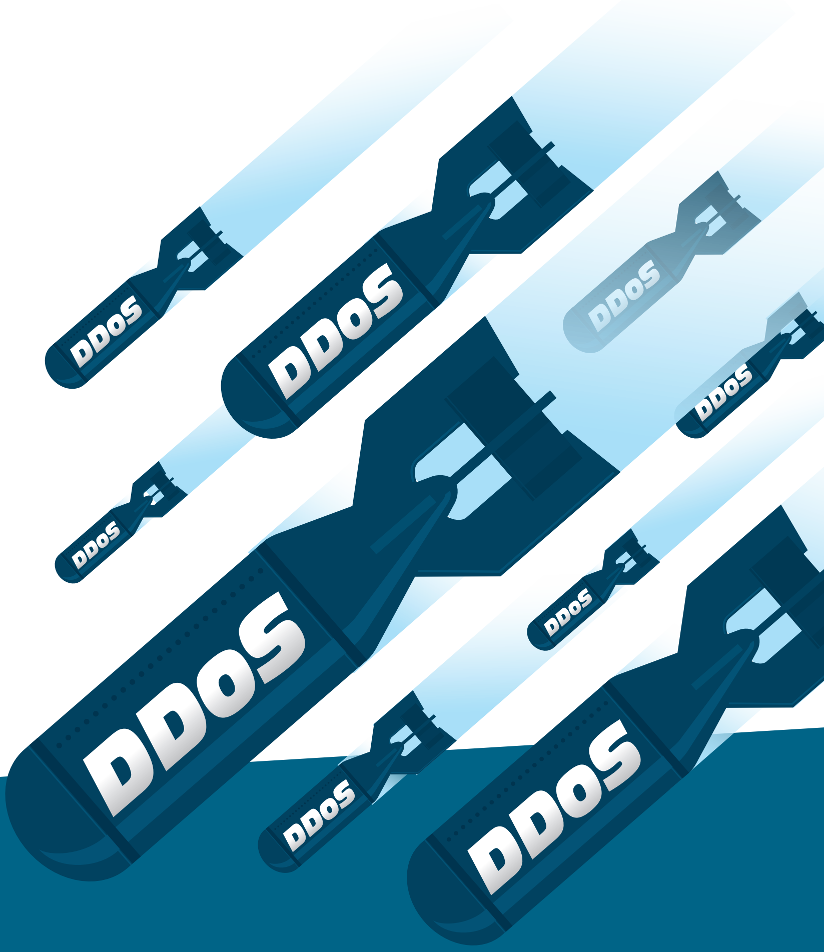
DISTRIBUTED DENIAL-OF-SERVICE

A DDoS attack is an acronym for a distributed denial-of-service attack. DDoS attacks can target anything connected to the Internet, such as networks, servers, devices, and applications.

During a DDoS attack, the attacker attempts to overload a server with fraudulent requests for data, rendering it unable to function normally. By doing this, an attacker employs all of the available resources so that it is unable to process authentic requests by users.

There are two types of DDoS attacks: one that sends fraudulent data or requests from a single source, and another that coordinates an attack from multiple systems to one location.

The second type of DDoS attack is much more common because attacks from one source are significantly easier to identify and thwart.



MALWARE

Malware is any unwanted software installed in your system without your consent and intentionally designed to cause damage to your computer, server, client, or network. Some of the most common types of malware include spyware, ransomware, viruses, and worms.

Viruses – A virus attaches to applications, code and files, executing viruses in the place of and replicating itself to do the same at other locations in a computer system.

Trojans – A Trojan horse maliciously hides in a useful program with the purpose of creating a back door that can be exploited by attackers. Unlike viruses, Trojans do not self-replicate.

Worms – Worms are self-contained programs, commonly spread through email attachments. When triggered, worms propagate across networks and computers spreading malicious activities than can lead to DDoS attacks.

Ransomware – Ransomware is a type of malware that blocks access to the victim's data and threatens to publish or delete it unless a ransom is paid.

MAN-IN-THE-MIDDLE

A man-in-the-middle cyberattack occurs when a hacker hijacks the communications between a client and a server. These attacks often go undetected because the two parties believe they are communicating directly with each other.

Man-in-the middle attacks use methods such as IP spoofing or DNS spoofing to intercept your Internet traffic and then decrypt it. IP spoofing impersonates the source of data they send to your computer, masking it as a trustworthy source. In a similar way, DNS spoofing hacks into your DNS resolver's cache and redirects you to a fake site.

PHISHING

A phishing attack is a practice of sending fraudulent communications that appear to come from a reputable source, usually through email.

The goal of a phishing attack is to gain personal information or influence a user to do something.

It could involve opening an attachment to an email that loads malware onto your computer or clicking on a link to an illegitimate website of which you hand over your personal information.

SPEAR PHISHING

"In a normal phishing attack, the attacker sends the emails randomly to convince the victims to open an email containing the attachments with the embedded malware or links containing a virus. However, in the case of spear phishing, the attackers send the emails to the specific targets." *(Source: Infosec)*

This type of attack combines social engineering and psychological manipulation to trick people into performing actions or divulging confidential information to a trusted source.

In the age of the Internet, you can find personal information on an individual in minutes. The attacker uses publicly accessible information to make their email plausible or to impersonate an individual or organization sending the email.

5 WAYS TO IDENTIFY A SPEAR PHISHING EMAIL

Although spear phishing attacks are very convincing in nature, there are a few ways to identify such emails. Following are the ways to spot the warning signs of a spear phishing email.

1. CHECK THE SENDER EMAIL ADDRESS AND NAME

If you are questioning the validity of an email, one of the first places to look for clues is the email sender address. Confirm that the email handle, domain name, and domain extension are all correct. An email address that has missing characters or additional hyphens and words is a common indication that something is amiss.

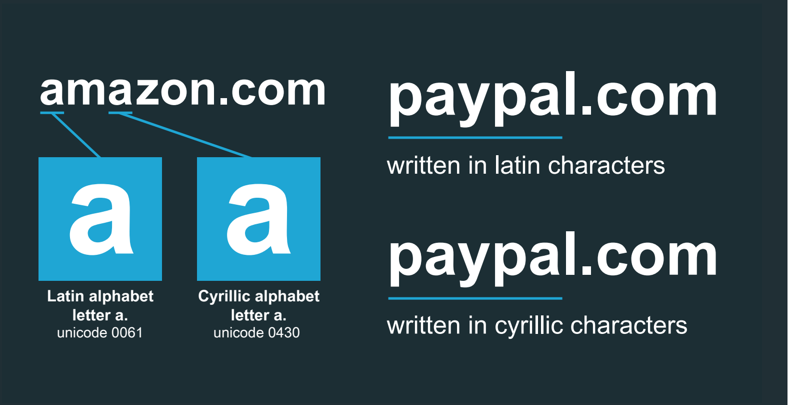
From: **Bank** <employee@card-alerts-bnk.com>

Sometimes, variations of the sender's address are so minute the untrained eye would miss them. Homographs are a typical example of this.

Homographs
When visually-similar letters from one character set are replaced with a letter from a different character set.

Examples of Homographs

paʏpɑ1
pɑypɑl
paypa1


amazon.com
a
Latin alphabet letter a.
unicode 0061
a
Cyrillic alphabet letter a.
unicode 0430
paypal.com
written in latin characters
paypal.com
written in cyrillic characters

2. CHECK THE EMAIL FORMAT AND CONTENT

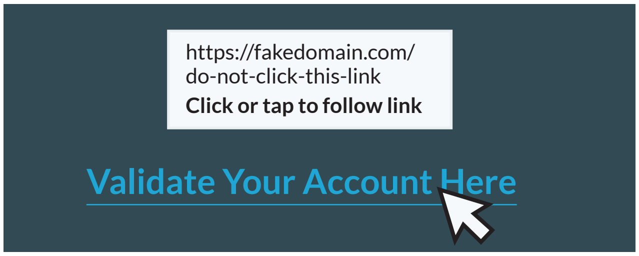
Although the attackers may be able to spoof the email address or name of an individual or organization you know or trust, the formatting of the email is often a giveaway. If you are unsure of the authenticity of an email, go back into your inbox and see if the email format matches the emails you received from that sender in the past.

Spelling and grammatical errors are also a tell-tale sign of a spear phishing attack. In the email, the author may confuse words like "advise" for "advice" or feature long and improper sentences.

3. VERIFY SHARED LINKS AND ATTACHMENTS

Many spear phishing emails will try to get you to click on a link where the attacker can hijack your web browser, install malware in your system, or get you to share sensitive information.

Luckily enough, there is a simple trick that allows you to see the complete website address of an embedded link in an email. Simply hover your mouse over the link, and it will show you the link path you will be redirected to.


https://fakedomain.com/do-not-click-this-link
Click or tap to follow link

Validate Your Account Here

If the web address looks suspicious, do not click on the link or any attachments. An attacker can spoof entire websites, so when in doubt navigate to your trusted website directly, or call to verify the legitimacy of the email you received.

4. QUESTION ABNORMAL BEHAVIOR AND REQUESTS

A spear phishing email is a well-planned attack that preys on emotion. So don't let it. Question abnormal behavior you see in the email. If something feels off, it probably is.

For example, if the sender asks you to do something in a way you have never done before, such as sending a wire transfer payment instead of physically mailing a check, you should be suspicious.

There is usually an underlying sense of urgency in spear phishing campaigns – don't let this shake your common sense or due diligence.

Be wary of any email that instructs or coaxes you to share sensitive information which is not supposed to be shared without proper consent.

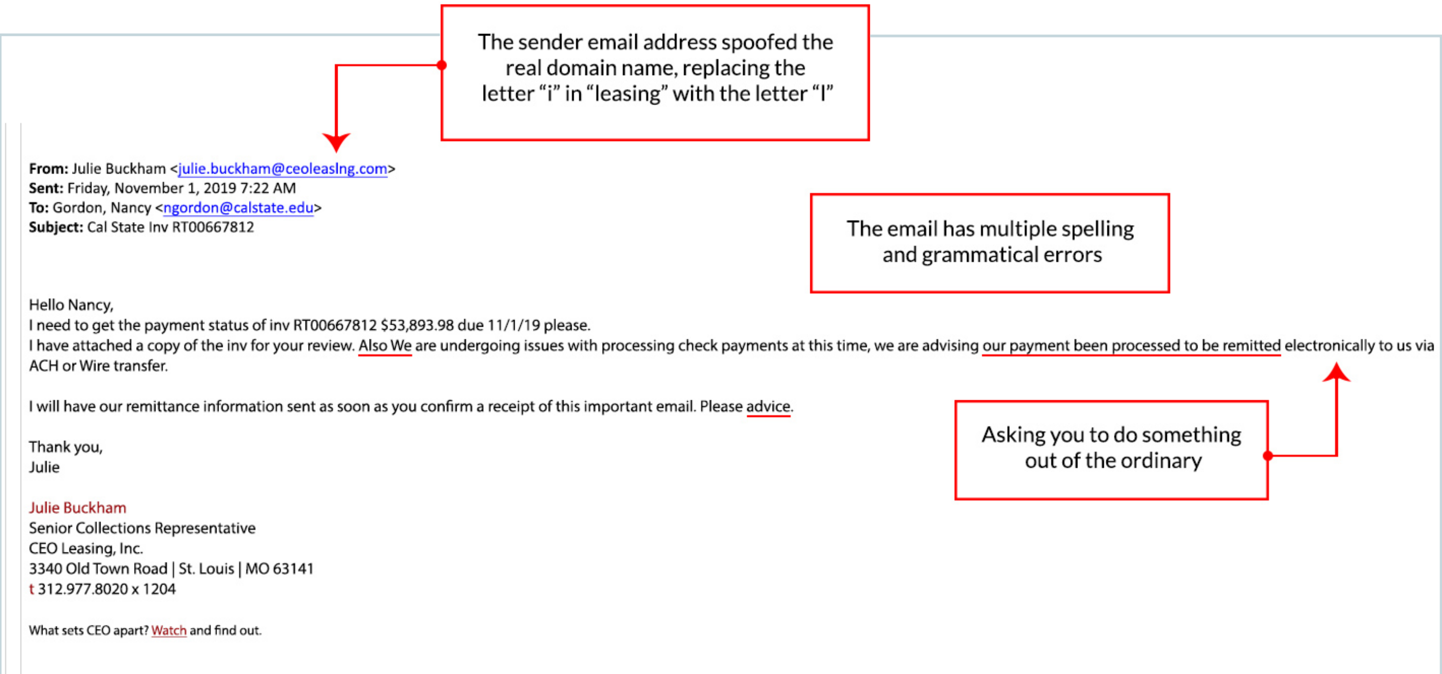
5. VERIFY THE EMAIL WITH A PHONE CALL

Last but not least, when in doubt, do not hesitate to call the email sender to confirm the authenticity of the email and information requested. Remember, you and your colleagues are the first line of defense for your organization.

Some spear phishing attacks are so inconspicuous you may not realize they are happening. Still, if you follow the precautions outlined above, you can prevent sensitive information from ending up in the wrong hands and causing enormous problems for you and your organization.

101DOMAIN CUSTOMER CASE STUDY

A 101domain customer who will remain anonymous, recently found themselves as the target of a spear phishing attack. You can see the initial email below in which the names and addresses have been altered for our client's protection.



The sender email address spoofed the real domain name, replacing the letter "i" in "leasing" with the letter "l"

From: Julie Buckham <julie.buckham@ceoleaslng.com>
Sent: Friday, November 1, 2019 7:22 AM
To: Gordon, Nancy <ngordon@calstate.edu>
Subject: Cal State Inv RT00667812

The email has multiple spelling and grammatical errors

Hello Nancy,
I need to get the payment status of inv RT00667812 $53,893.98 due 11/1/19 please.
I have attached a copy of the inv for your review. Also We are undergoing issues with processing check payments at this time, we are advising our payment been processed to be remitted electronically to us via ACH or Wire transfer.

I will have our remittance information sent as soon as you confirm a receipt of this important email. Please advice.

Asking you to do something out of the ordinary

Thank you,
Julie

Julie Buckham
Senior Collections Representative
CEO Leasing, Inc.
3340 Old Town Road | St. Louis | MO 63141
t 312.977.8020 x 1204

What sets CEO apart? Watch and find out.

THE ATTACK

Our client, let's call her Nancy, was so convinced of the email's authenticity she responded. However, instead of complying with the demands, she first questioned the request asked of her. Based on the responses she received, Nancy was suspicious of the legitimacy of the email and forwarded it to a colleague in her organization. Let's call him Steve.

Steve sent the email to a different employee at the sender's company, in addition to calling them directly to discuss. In the email that he forwarded to the real company, Steve warned them not to click or open unknown links or attachments. Quick thinking Steve!

Together, the two organizations were able to conclude that the email was a scam, and thankfully no sensitive information was shared in the process.

Other clients of ours have not been as lucky. We even had a case earlier this year, in which our client, a bank, wired money to a spear phisher. By the time they had realized the email was an attack, it was too late.

SAFEGUARD YOUR EMAIL INFRASTRUCTURE

Being able to identify a spear phishing email is a great help in reducing the risk of falling for an attack. Still, there are additional measures you can take to protect your organization, employees, and digital assets.

The domain name system controls many services we rely on for connecting and communicating on the Internet. When you send an email, it is important that the message arrives at the receiver. It is just as essential that emails arriving in your receiver's inbox with your name on them, are actually being sent from you.

There are a few records you can add to your DNS settings that will improve your email deliverability and reduce spam: SPF, DMARC, and DKIM.

SPF

A Sender Policy Framework (SPF) record indicates which mail servers are authorized to send mail for a domain. Before an email arrives in an inbox, the recipient's server performs a check to verify that the email is coming from an authorized server.

DMARC

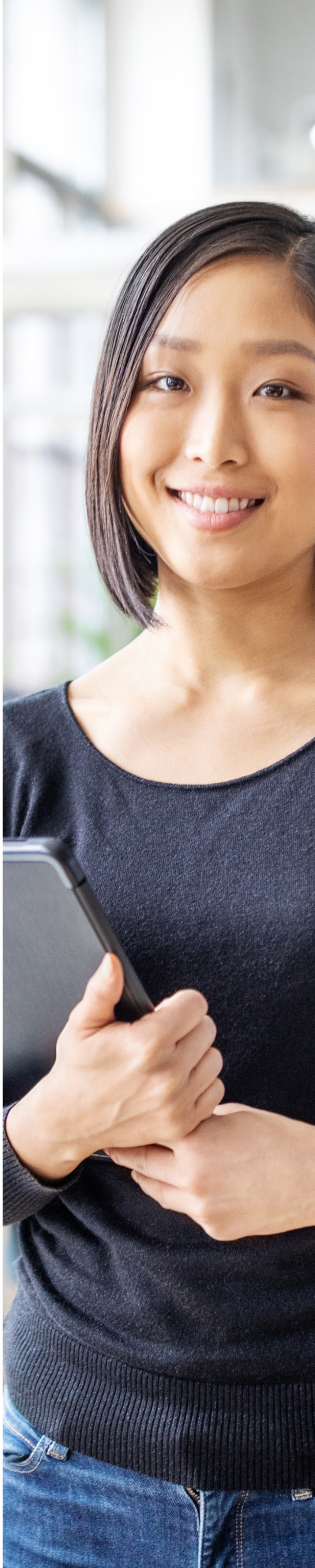
Domain-based Message Authentication, Reporting & Conformance (DMARC) is another record type that builds on the collaboration between senders and receivers to reduce spam.

Receivers specify to senders how they authenticate emails, and the senders tell the receivers what to do with mail that does not pass the verification. DMARC's authentication practices enable receivers to reject unauthenticated messages.

At the very least, every enterprise should have SPF and DMARC records. The third record is less crucial but still a safeguard none-the-less.

DKIM

A Domain Keys Identified Mail (DKIM) record adds a digital signature to emails. The recipient's server will check that the signature is associated with the correct domain. This type of check ensures an email has not been modified in transit and is a powerful resource to prevent man-in-the-middle attacks.



PROTECT YOUR SITE FROM CYBER ATTACKS

Your website is a significant touchpoint for your business. It's how customers find and interact with your brand online, which is why it is vital that it works quickly and stays online at all times.

Every second your website is down means money down the drain. Cyber attacks aim to bring your site down and compromise sensitive customer data. A single data breach could tarnish your brand reputation and put you out of business.

A standard DNS service is no longer good enough. Enterprises require a premium DNS service that is scalable, easy to use, and integrated for security and performance.

Trusted by over 20 million websites and webmail properties, Cloudflare is the security solution that is helping build a better Internet.

CLOUDFLARE® SECURITY BENEFITS FOR ENTERPRISES

DDoS Mitigation

Cloudflare combines multiple DDoS mitigation capabilities into one service to keep applications, websites, and APIs highly available and performant.

Anycast Network

Cloudflare observes 15% of global Internet requests across 194 data centers and can defend against the largest and most sophisticated attacks.

Data Breach Prevention

Prevent attackers from compromising sensitive customer data, such as user credentials, credit card information, and other sensitive information.

Bot Management

Block abusive bots from damaging Internet properties through content scraping, credential stuffings, fraudulent checkout, and account takeover.

PARTNER WITH A PARTNER YOU CAN TRUST

With increased pressure for security on the Internet, customers are only choosing to give their business to companies they can trust. Luckily enough, achieving a secure infrastructure for your digital assets does not have to break the bank.

Training your employees to identify spear phishing costs you next to nothing. Adding pertinent records to your DNS settings requires little effort. Investing in your website's performance and security is simple and cost-effective when you join Cloudflare's CDN network.

If you would like more information or advice on how to implement any of the security features mentioned, 101domain dedicated account managers and experienced engineers will be happy to assist you.

101domain.com Corporate Brand Services

www.101domain.com
corporate@101domain.com
877.983.6624