DRUVSTAR

How to Protect Yourself and Your Company from Phishing for Free

We all receive weird emails that don't seem quite right. Spam, sales, offers, and the like. Interacting with some of them poses a real threat – these are phishing emails.

According to the FBI, phishing was the most common type of cybercrime in 2020—and phishing incidents nearly doubled in frequency, from 114,702 incidents in 2019, to 241,324 incidents in 2020. 75% of organizations around the world experienced some kind of phishing attack in 2020

But what is phishing, how dangerous is it really, and what can you do to protect yourself for free?

Table of Contents

Part 1

INTRODUCTION

What is your top cybersecurity priority?

Even though vulnerabilities that affect many devices at once often have catchy names like SolarWinds supply-chain attack, Heartbleed, or Kraken, your number one risk still comes via your employees. Their email and device are the weakest points and prone to phishing. If you can reduce your exposure here, you can drastically reduce your business's level of security risk.

95% of attacks are made possible through mistakes made by people, which may seem counterintuitive. Zero-day vulnerabilities might still get all the press, but as software engineers get better and security measures mature, it also gets much harder for hackers to work than it was ten years ago. Human behavior on the other hand takes a lot longer to change.

The market rate for revealing major zero-day secrets is astronomical. unfortunately, the only groups that can afford to buy these discoveries from hackers and exploit them are often tied to nation-states.

Phishing attacks are easier to carry out than a multi-step software-hacking campaign. There are many more hackers that are willing and capable of executing a break-in by hacking **not software but humans.** This translates to an ongoing broad barrage of phishing attempts across the globe.

Real-World Numbers

In my previous incarnation as a tech employee, I remember my Head of IT using the KnowBe4 product to emulate phishing attacks across the business. He followed up each round with targeted security training based on the results of the test attack.

During the first phishing round, an astonishing 50% of the employees clicked the malicious link in the fabricated email. And 35% gave away their user credentials! Luckily for the business, that was a test. But it was clear that we needed to remediate this immediately. With such results of a simple test, what were the chances that the company's infrastructure wasn't already at the full disposal of real malicious actors?

A Quick Definition of Phishing

Phishing is a type of social engineering attack that uses technical means of communication to trick the victims into handing over personal information, exposing their work credentials, or downloading malware on their personal or work devices.

Phishing uses emails, phone calls, texts, or instant messages sent out to individuals across organizations or personal inboxes and devices. Cunning social engineering techniques are used to encourage the victim to click a link, fill out a form, enter a password, or open an attachment – and any of these actions can compromise the organization's systems.

Such messages or files may appear to come from a trusted source, but if you know what to look for, you can spot phishing and avoid getting tricked.

Part 2

WHEN THE SENDER IS AN IMPOSTOR

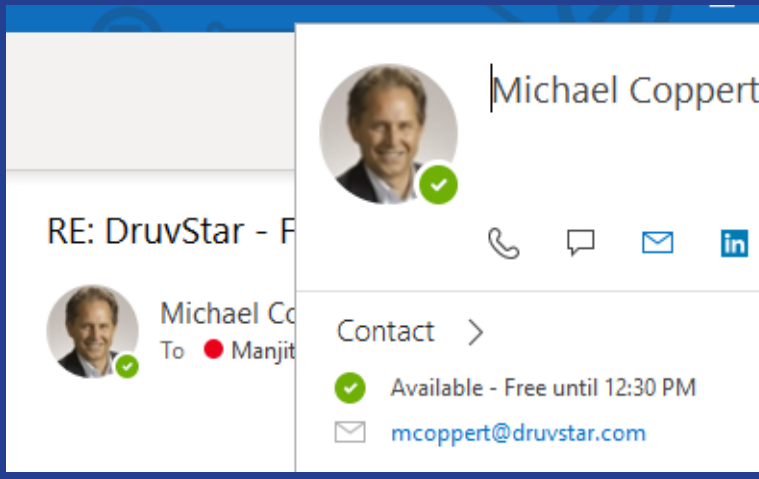
In "spoofing", attackers want you to think they're somebody else: preferably someone you trust or respect. It's easy for anyone to establish management and employees in a company. A quick browse of the company's website, LinkedIn page, shareholder report, or numerous other publicly available online sources can provide a wealth of information. Attackers will use it to hide their true identity by assuming somebody else's identity and try to encourage you (or your employees) to do their evil bidding.

Your email infrastructure admins should configure your email service to tag the external emails (preferably using bold red letters). This will clearly show the receiver that the email didn't come from within the company's infrastructure, naturally creating small pause in their follow-up action. This sub-second pause is amazingly effective in slowing the rate of phishing attacks.

Check the Sender's Email Address

Always check the sender's email address, not just the displayed name. Watch out for misleading URLs (more on URLs later). Each email application is different, so check how to view the complete "from" address in your email application.

For example, in Outlook Desktop, you can hover your mouse over the "from" field and then over the envelope. In the image below you can see that the sender was Michael and used the account **mcoppert@druvstar.com** (Michael is DruvStar's VP of Business Development).



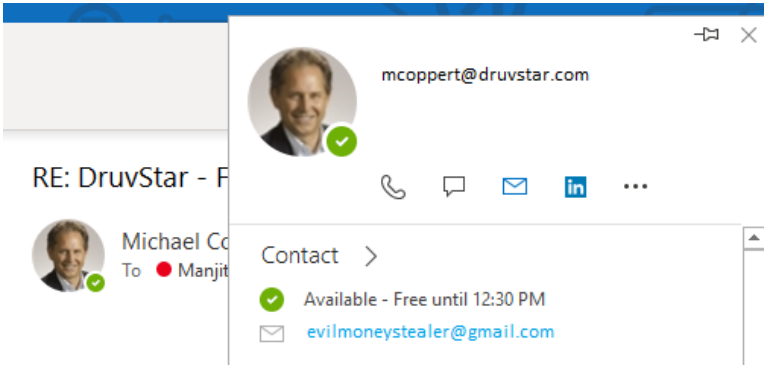
If the address line isn't what you would expect, then don't go any further. Delete the email or report it to your IT department.

The Name Field Can Be Replaced With Anything

Watch out for the name field that looks like an email address. For example, below, you can see that instead of the name "Michael Coppert", the "name" field now features "mcoppert@druvstar.com". You must learn how to look for things like this and know the difference between the "name" and the "email" fields. Remember:

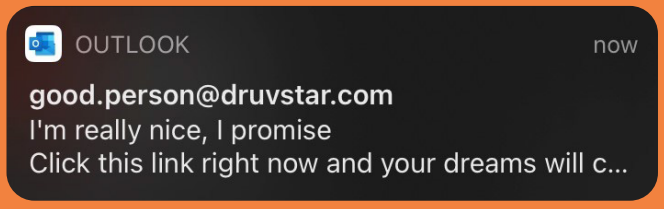
- The "name" field contains the sender's name and
- The "email" field contains the sender's email address

Attackers can easily update the "name" field when sending an email to make it display anything they need to display. Hackers can be very clever with this. Double-check the sender's email address. For instance, in the screenshot below, it's "evilmoneystealer@gmail.com".



Mobile Devices Make It Harder to Check

Take your time when reading emails on mobile devices since they will truncate what's displayed. It's easy to get caught out when you don't see the full picture. For instance, consider this actual screenshot from my phone. I sent this using my personal Gmail account that is in no way related to DruvStar.



From the way it is displayed on the mobile device, it may make you think that this was sent by somebody called "Good Person" who works at DruvStar, but since you are only seeing the name field and not the origin email address, you are easily deceived.

Check with your provider on how to display and check the actual sender's email on your device in the email client you're running.

Part 3

DODGY URLS

This part breaks down the URL tricks and shows you some examples of how URLs can be misused and faked to trick an unsuspecting user. This chapter might get a little deep into the tech details, but stick with it and read it thoroughly – it's worthwhile. Security of your company (and your private data) is at stake here.

URL (written in full as "Uniform Resource Locator" – now you can impress somebody with this knowledge) is a website address. It usually consists of several obligatory and some optional parts. The resulting combination can be somewhat hard to understand.

Let's examine this by breaking down two example URLs:

https://www.anorganization.com/path/path/page.html#placeinpage

and

https://www.anorganization.com:8080/path/endpoint?param1=123&param2=456

HTTPS	This is the scheme (or sometimes called the protocol) The "s" in HTTPS stands for "secure". Always make sure that your browser agrees and shows a locked padlock icon next to HTTPS in the address bar. Other scheme types that you might see are HTTP, FTP, file, etc. For regular web surfing, you'd generally want to see and use HTTPS since this protocol doesn't only provide secure communication, but also allows your browser to validate the site itself. If you've got some time to kill, you can check out the full list here: List of URI schemes - Wikipedia.
://	A divider between the scheme and the hostname of the website hostname.
www.anorganization.com	The hostname of the website.
.com	Top-Level Domain (TLD) (also known as domain extension). Other examples include .edu, .gov, .org, .co.uk, .io, .net, and a myriad of other variants (fun fact – every country has its own domain extension, even the long-defunct Soviet Union – .su). The current list of TLDs is here: List of Internet top-level domains - Wikipedia.

anorganization	The domain name. This will generally represent the name of the organization.
WWW	Stands for the "World Wide Web". And in this case, is called the third level domain. The third and higher levels are optional and can represent different environments within the primary domain. For example: • anorganization.com (the third level is left out entirely) • dev.anorganization.com (no www, but points to a dev location) • www.staging.anorganization.com (third and fourth levels are included)
:8080	This is a port number. It will nearly always be left out since HTTP defaults to port 80 and HTTPS to port 443. If you see anything like this in URLs that you're not regularly using for work or for configuring some of your personal hardware, be wary.
/path/path	Subdirectories on the site. They navigate to web pages in folders.
Page.html	The content that is served to the user. Sometimes you may not see a page name but rather just the paths. This is generally ok.

#placeinpage

Allows a link to point and take you directly to a specific marker within a web page.

?param1=123&param2=456

Sites can pass information via URLs (and behind the scenes, through JavaScript and WebSockets).

- The "?" indicates that some information is being passed
- "param1" is the name of the information
- "123" is the value being sent

Multiple parameters are sent using "&" to join them together.

Remember, it is critical to be able to recognize and tell the difference between the top-level domain (.com) and the domain name (anorganization). These – together with HTTPS – will give you the confidence that the website you're visiting is what you expect it to be.

Now that we've learned how to understand the contents of a URL, let's see how attackers exploit the average user's lack of knowledge.

Website URL	Security evaluation
https://www.anorganization.com This is a valid site that is safe to visit if that's the site you were looking for.	GOOD
http://www.anorganization.com/anorganizationthingythingy Same website, but with two changes: • The path added here is fine since this is still in our trusted anorganization.com's domain. • However, the scheme is "HTTP". This generally isn't a bad thing, but if you can go directly to the HTTPS version, do it for safety's sake. • Never enter information into a site with HTTP. It's not secure and can be snooped by anyone in any network in transit.	OK/BAD
https://www.anorganization.org Watch out! Often organizations will scoop up as many top-level domains (TLDs) as possible (the .org bit) that match their organization name, but not all companies can get all TLDs. Suppose you go to www.microsoft.vegas, you will get redirected to Microsoft-.com. But yahoo.vegas doesn't exist and could be bought out by hackers to be used as bait. This means that an attacker could place an exact copy of a trustworthy website there.	BAD

Website URL	Security evaluation
It will look secure, and when you enter your credentials, you'll see what you expect to see on a legit website. But by doing so, you'll provide your personal, work, or banking information to a bad actor. What's worse – you probably won't spot the mistake/identity theft for some time, sometimes until the hackers use the information you provided.	
https://www.anroganization.com Check the spelling. Bad actors will try to pull the trick described above, but with common typos to place their copycat websites there.	BAD
https://www.anorganization.com/somelocation?param1=123xyz&param2=xyz123 Some parameters are passed in the URL, but it doesn't look suspicious. This is still a valid URL of a trustworthy website.	GOOD
http://www.anorganization.123.com This is a widespread scam method. At a glance, the "123" looks like a part of the "anorganization" domain, but that's not true. The domain here is "123.com." – anorganization is just a third-level domain name on that server.	BAD

Website URL	Security evaluation
http://www.anorganization.corn That cunning attacker! Can you spot what's wrong with this url? Look closely at the top level domain.	BAD
https://www.anorganizationsecurity.com This is quite a common and popular way to trick people – adding some seemingly legitimate part to a brand/website name to create a whole new domain name for copycat websites.	BAD
https://www.anorganization1.com Anything added to the domain name within the domain name itself is not just bad – it's a different website name altogether. For example, the "anorganization1" is an entirely separate domain from "anorganization.com", and anyone could have registered it.	BAD
https://www.microsoft.com/en-us/microsoft-365/business/compare-all-microsoft-365-business-products-b This is a genuine Microsoft link – all the different path elements look a little crowded, but it's all fine.	GOOD

Website URL	Security evaluation
https://www.microsoft.com.en-us.microsoft-365.busines-compare.com/all-microsoft-365-business-products-b This trick exploits the compound nature of the real enterprise links of a company like Microsoft. It looks OK at a glance, and it's tempting to scan a long URL, decide that it seems legit, and click it. But, unfortunately, that's precisely what the evil **business-compare**.com wants you to do.	BAD
https://www.anorganization.com/ This link would look perfect inside an email or a document – however, if you hover the cursor over it, you'll see that it points to https://www.google.com. This can be challenging to spot if the link is also very similar to the actual website address it's supposed to lead to.	BAD
HTTPS://WWW.G00GLE.COM Capital letters are ignored in URLs, so that's not a problem. The problem is that here the capital letters are used for hiding zeroes instead of "o"s in this URL.	BAD

The best way to avoid getting "pwned" (a hacker slang for "tricked; something or someone a hacker has received full access to") is never to click links in an email that you have any shadow of suspicion. When in doubt:

- Go directly to the company's website
- If there's a path beyond the domain name, add it in the browser's address bar manually
- Double-check the domain name
- Leave out any parameters unless you're sure you need them

You can also do a right-click (or Ctrl-click on Apple), copy the link from the email, and then paste it into a text editor that doesn't support hyperlinks (something like Notepad will do). This way, you'll know that the link is what it appears to be. Using your simple text editor, you can verify or delete anything extraneous and then copy and paste the link into the browser.

Part 4

THE PSYCHOLOGY OF CONTENT

Before proceeding, let's do a quick recap of what we've already learned:

- You now know how to spot and avoid an email that pretends to come from someone you trust
- You can spot a bogus URL
- You now know that it's better to avoid clicking dangerous links, which helps protect you from giving away credentials

You're already in pretty good shape security-wise!

Now, let's discuss how an attacker can get inside your head by hacking the reader using psychological tricks in the email content.

The Boss

If you get an email from your boss, or your boss's boss, who tells you to review something urgently, what will you do?

When seeing an email like that – even though it might seem a phishing attempt – you are inclined to keep nervously looking at it again and again before hitting the Delete button. The subconscious mind is panicking – "but what if it is really her and she needs this urgently?"

A message from a fake "boss" could ask for something simple but meaningful:

- "Could you review this document?"
- "Can you take a look at this site and provide your feedback in the next 30 minutes?"
- "I've decided to promote you. Fill out the attached HR form."

You already know that you need to check the sender's name and the URL, but what if your boss has already been hacked and the message was sent using their legit email account? How do you spot this if the URL, return email, and everything else also looks good? Ask yourself this:

1. Do you normally get emails from them?
2. Are they saying something strange? Like, "Hey Andrew, I lost your phone number. Can you re-send it to me, please?"
3. Are you letting pressure or excitement in the email distract you?

When in ANY doubt, communicate with the sender through another channel to verify their request. Pick up the phone and call their known number (not one that's been sent to you in the email) or reach out to them via known messaging channels.

The IRS, Social Security, et al.

Picture this – the IRS has reached out to you via email sent from **1RS.org**. They tell you that something went wrong with your filing. It is almost evening, but, you can still resubmit it via **IR5.org/latesubmissions.** However, you must do it today or pay a hefty fine. Nobody wants to be on the wrong side of the IRS, and calling them to verify can be very challenging, especially if it's the end of the day.

URL verification should help with these. Don't click the link, but rather go to the actual IRS website. Try to navigate to the "late submissions" page. If that page exists, then it's time to sit on the phone for a while with the IRS to find out if they contacted you.

Friendly Reminders

By doing some light investigation on a specific phishing target, the attackers can make the email more personal and entice the individual to respond. For example, if they know that you were at a conference, webinar, or other events, then they can get very believable and accurate with details.

From:

REG@CYBERSECUR1TY.COM

"Hey Nancy, I just realized that I didn't follow up from our discussion on cybersecurity at CyberCon last month. Here's that link to the content I promised to forward."

Remember not to click links in emails like this one!

Urgency

Watch out for urgency in emails. Phishing messages will often say that you need to do something that very moment, as soon as possible. It's almost too late, the princess is tied up, and the dragon's about to eat her.

The reason behind this urgency is that if you take a minute to think about the request or talk to someone else, you will likely uncover the fraud, so the attacker needs you to act right now.

It's a Secret

There are many times when one can reasonably expect confidentiality in business, but this is also a tactic exploited by the bad guys. If you can't tell anyone about the email, your chances of spotting that it's a phishing attempt decrease. Good for the bad guys, but bad for you. Again, verify the source and talk to the sender before taking any actions.

Part 5

TYPES OF PHISHING

As the hacking world has matured, so has the cybersecurity industry. This maturity has come with a slew of vocabulary and acronyms that try to group and define this new environment. Sticking to the "Phishing" topic, let's go through the "Phishing" glossary.

Spear-Phishing

A subset of phishing where the attacker knows something about the target. For example, you can get a phishing email that appears to be from your manager. In contrast to the mass-sent Social Security and DMV fraud phishing emails that tend to be non-personalized, this attacker knew who you are, what organization you're in, and your manager's name.

Spear phishing emails now represent over 90% of all phishing attempts because they are generally much more successful for the attacker.

Smishing

Smishing is short for SMS-phishing. SMS stands for Short Messaging Service, which we usually call "texting". Since smartphones and some featurephones recognize and process links in text messages, SMS is now a great place for attackers. They can send a malicious link to your phone number, and once you click it, it will take you to a website that looks like a familiar one.

For example, yesterday my wife received a few text messages which looked a bit like these:

- "Facebook PR: #Unauthorized page usage #We received an Abuse Report against your page. #Log in via link and review: https://-facebook@bit123.ly/something"

- "(Notifications Facebook) Dear Customer, we removed your Facebook post because it contains abusive content, visit https://face-book-login-attemp-support.farmacias-mooper.com"

If you try to log in using such links, you'll hand your credentials over to a criminal. Once they get your Facebook password, they can quickly download everything about you and all your friends, which in turn improves their ability to target people on your friend list directly and pretend to be you.

Clone Phishing

The attacker takes a genuine email and responds or forwards a message under the guise of the original sender (or receiver) but changes links, attachments, content, etc. The link description may also remain the same, but the underlying link could be nefarious. The new sender credentials are also often spoofed.

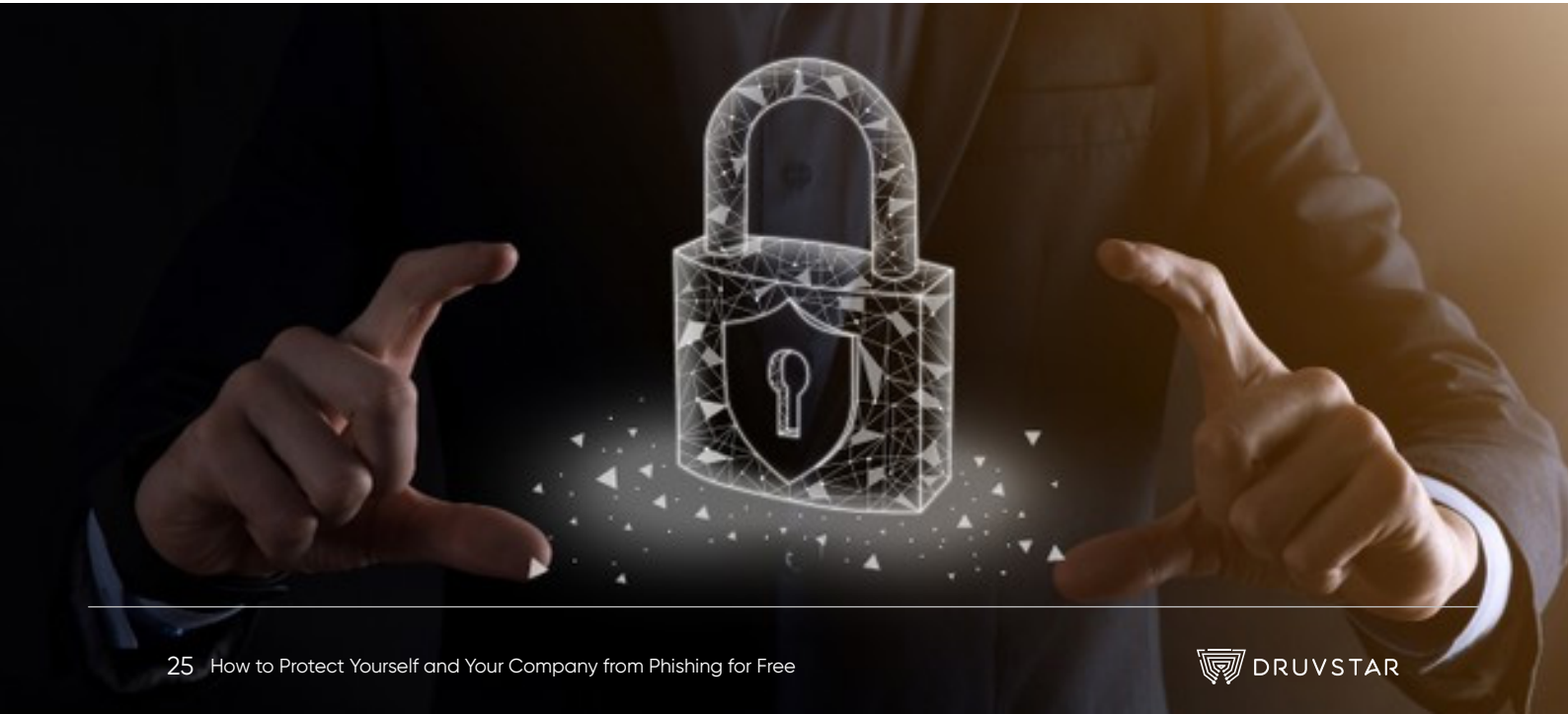
I'll admit that I used this method to prank one of my coworkers back in a day. How did I do it? I replied to an email he had sent weeks before. However, I completely changed the original email content, replying that I thought someone had used his computer to send a joke email.

But, of course, the reverse was true, and nobody had messed with his email but me. That email looked exactly as if it had come from him – because it had, only with completely different content.

Such a prank would, of course, get you fired today and probably should have then. But the point is – this is how clone phishing works.

How do the attackers get the original email to work with?

- They get it directly from either the sender or the receiver.
- They create an account to receive marketing or sales responses from the future victim.
- They may have already penetrated the network in other ways, and now they could have
  - compromised the email database,
  - set up new forwarding rules, and/or
  - created a dump of emails that they could later utilize.
- Once the attackers have the credentials and permissions they need, they can keep coming back to "drink from the well". Sometimes years later.



Whaling

Going for the big phish! Attackers prefer targets with high levels of access, authority, or trust. If they manage to breach such accounts, then they get almost unlimited access to the organization. These targets include heads of IT or security-related departments, C-level management, executives, and executive assistants. The latter tend to have access to their bosses' email and calendar, making them great easy targets.

Trust and authority are critical to playing social engineering tricks on other employees of the same company or its partners. The compromised executive account makes it very difficult for an employee to tell that the email is an attack and, if you're lucky, leaves them guessing whether to follow up. Most will fall prey to such an attack, especially if the attackers know human psychology.

Leaders of IT departments tend to have high levels of permissions, which could mean direct access to critical assets and private information. This risk can be mitigated by solid role management principles, including:

- least privilege access
- multiple accounts
- checks and balances
- multi-factor authentication (MFA)

and others that are beyond the scope of this paper.

Vishing

Voice-phishing is all those phone calls we take on our home, office, or mobile phones. The most prolific (aka annoying) for me at the time of writing this are the fake: DMV, car's warranty sellers, Social Security Administration, IRS, and tech support for all kinds of random IT services I'm not subscribed to.

These attackers use the same tactics, but they use voice instead of emails or SMS to trick us. And since these calls are live communication conducted by a real human being, they can be skillfully dynamic in their response and escalate tension and urgency with artistic ease.

Just hang up on them. If you worry that the call might be the real deal – still hang up and call the institution they claim to represent directly. You should know that with the help of call spoofing, the attackers can also make their incoming phone number look like a phone number of somebody you know. So please don't believe them. Hang up and call back to that person directly.

Throughout all these categories of phishing, the underlying tactics remain the same. If you know what to watch out for, you are in the best shape to protect yourself and your organization.

Part 6

WHY DO PHISHERS PHISH?

Attackers are normally looking to:

- Get valuable information from your company's systems or
- Obtain your personal and banking information

A few ways they can profit are from:

- Receiving ransom money by holding your data hostage
- Getting access to business or individual financial accounts
- Stealing, selling, or replicating your company's intellectual property
- Stealing or infecting your source code with malware
- Having early access to confidential financial data
- Blackmailing individuals or businesses

Just Kids

Very rarely is phishing used to do just some random damage. Although sometimes that's exactly what happens as the result of phishing. Such cases are the work of young or beginner hackers, also called "script kiddies", who cut their teeth in the hacking world using ready-made scripts and malware. After all, social engineering and phishing are the easiest ways for a hacker to get in.

Waiting Game

Phishing takes little effort (compared to software hacking) and can be propagated widely. Once victims have been tricked into giving up their credentials, the attacker can send emails posing as these victims and can do anything on the network that the victims have the rights to.

What's worse, phishers can use certain techniques (from lateral movement to using your account for Whaling) to gain escalated privileges to expand the area of their access.

Sometimes the bad guys will instantly go for what they want. However, they will often lurk around your account and systems to propagate as much as possible. This is when your information security partner should be able to detect and stop them.

Final Words

To successfully avoid phishing, you must be skeptical and question everything.

It's better to err on the side of being paranoid rather than careless. Consider every link or attachment to be a phishing attack – guilty until proven innocent. If in doubt, escalate through your company's policies or just reach out directly to the sender.

You might say that "That's too much work."
Cleaning up the mess and mitigating the damages when everything goes wrong is way more work than that, and rather unpleasant.

The biggest bang for the buck most companies get for securing their environments come from preventing phishing. However, despite all the training and communication paths, attacks continue to occur. DruvStar provides comprehensive threat management and vulnerability discovery services to harden your environment and to discover and respond when attacks occur.

DruvStar provides B2B cybersecurity around threat management to strengthen businesses across attack vectors. Using advanced technology solutions and our Las Vegas based Security Operations Center, we identify and combat security threats and strengthen our clients' systems and staff capabilities.

DruvStar solutions include:

Threat Management

- Security Operations and Automated Response (SOAR)
- Managed Detection and Response (MDR)
- Security Incident and Event Management (SIEM)

Security Vulnerability Discovery

- Penetration Testing
- Dynamic Application Security Testing
- Mobile Application Security Testing
- Live Threat Assessment
- Vendor Assessment
- Incident Investigation

Security Training

- OWASP Top 10 Issues
- Ethical Hacking and Countermeasures
- Security Awareness for Finance Professionals
- Security Awareness for Customer Service agents
- Incident Handling