BitDam

The Phisher’s Playbook

To protect yourself from them,
you must understand them

The Phishing Landscape

Much like in the wild, the phishing landscape consists of predators and prey.

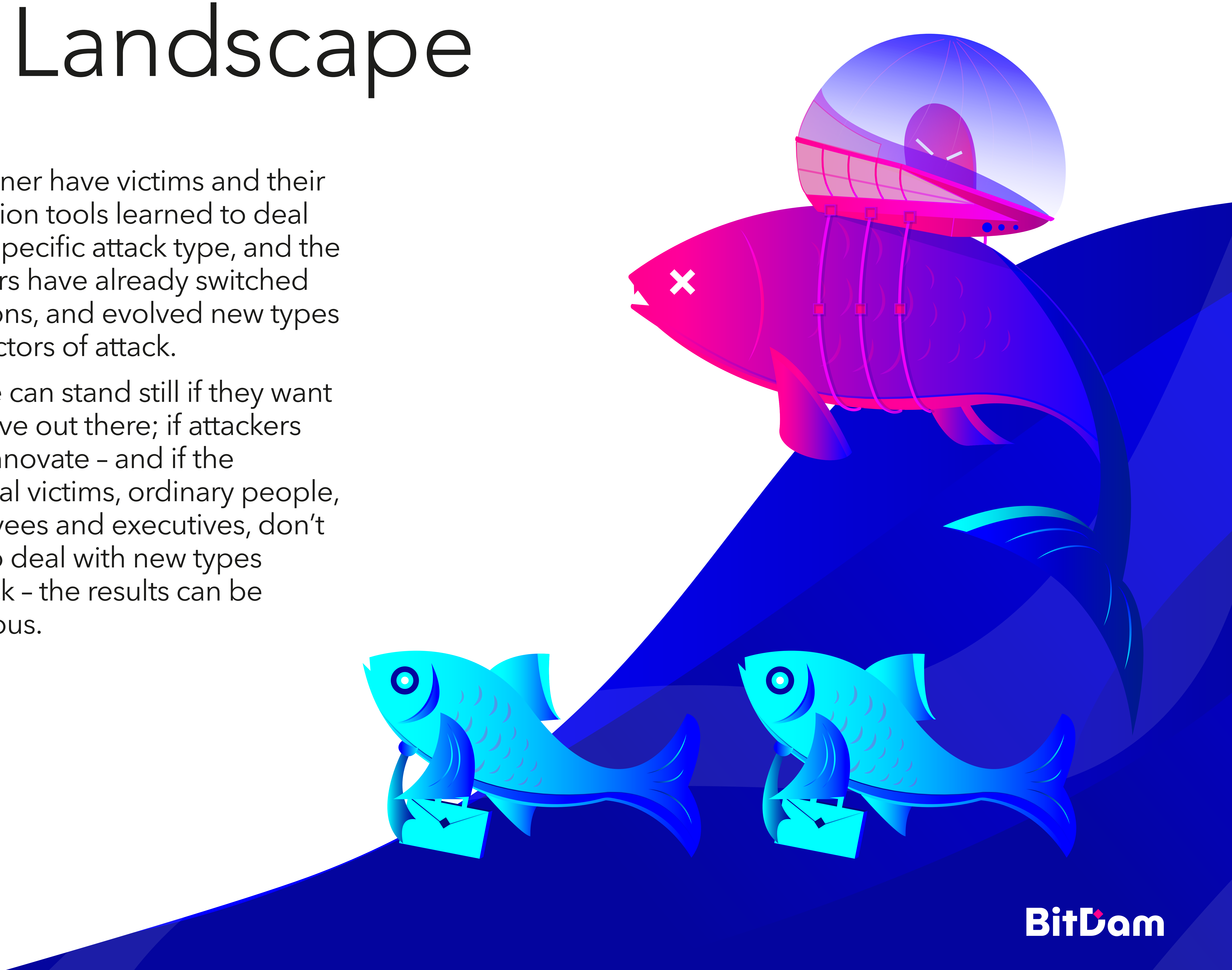
The predators are threat actors, constantly on the lookout for innocent victims, taking advantage of their quarry when they least expect it. The prey are ordinary people, going about their jobs and lives, doing their best to achieve their goals. They are not expecting or prepared for the attack when it comes.

The stakes are high, and it's often winner-takes-all.

This dramatic scene is played out thousands of times every day, across the globe.

No sooner have victims and their protection tools learned to deal with a specific attack type, and the attackers have already switched directions, and evolved new types and vectors of attack.

No one can stand still if they want to survive out there; if attackers don't innovate – and if the potential victims, ordinary people, employees and executives, don't learn to deal with new types of attack – the results can be disastrous.



BitDam

In This Playbook

In this Playbook we delve into the phisher's mind. Why and how they carry out their attacks, and what you can do to stay out of their clutches.

- What is Phishing?
- Into The Mind Of The Predator
- What do attackers want
- The Hunt
- Carrying Out The Kill
- Details Matter
- Mind Games
- Subterfuge & Camouflage
- Making the Escape
- The Future of Phishing

What Is Phishing?

Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details, by disguising oneself as a trustworthy entity in an electronic communication.

A typical phishing scenario:

1. Someone gets an email that they need to log in to their Office 365 account, from some made up reason
2. Clicking the link in the email leads to a fake Office 365 login page which looks exactly like the real O365 login page
3. The user inputs their login credentials, unknowingly sending them straight to the attacker

96%

of phishing attempts use email as the primary delivery vector

65%

of organizations in the US experienced a successful phishing attack in 2020

Into The Mind of The Predator

How does the attacker think? What's going through their mind?

How do I maximize my income while minimizing my risk?

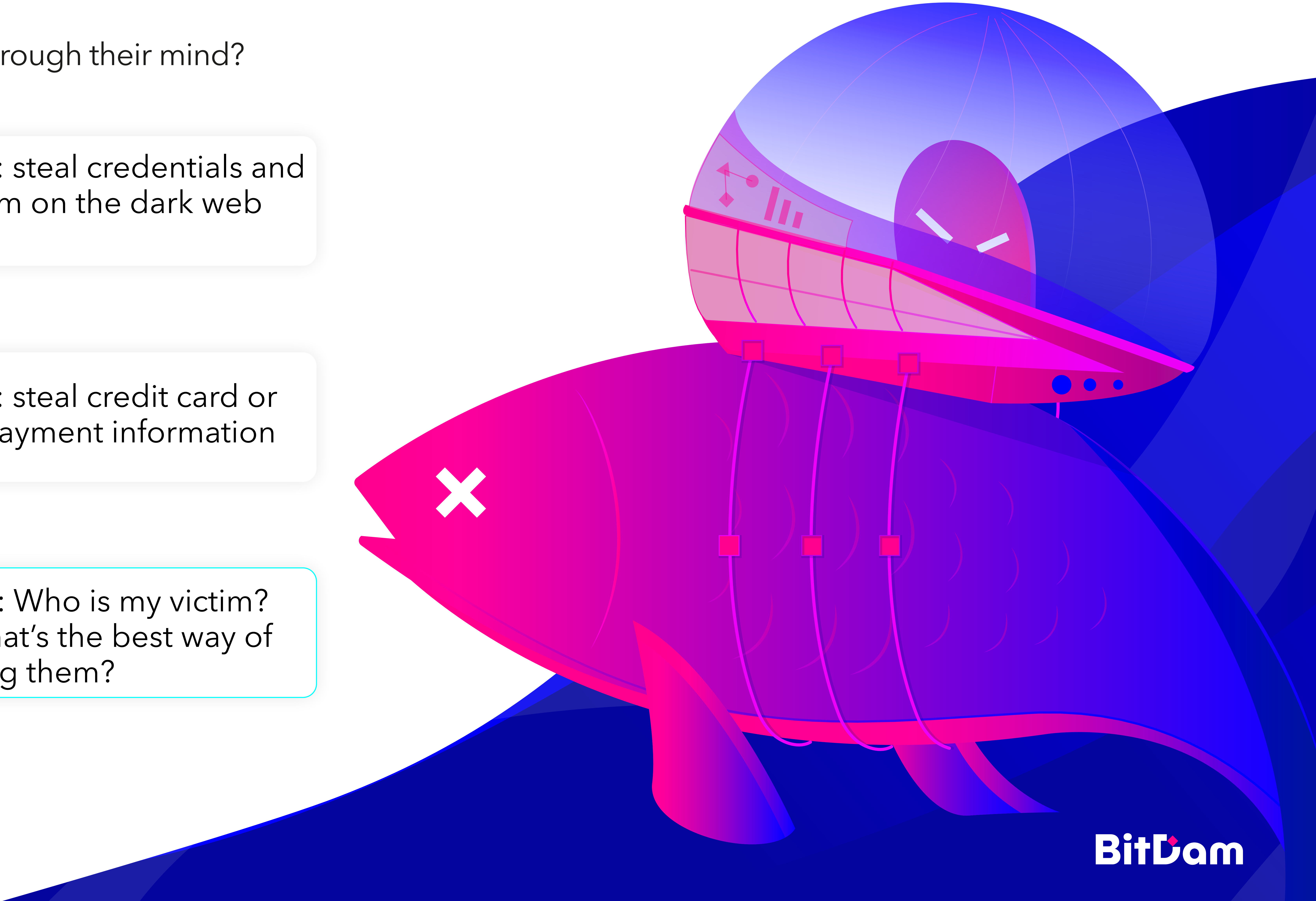
Option: steal credentials and sell them on the dark web

Option: steal IP and sell it to competitors

Option: steal credit card or other payment information

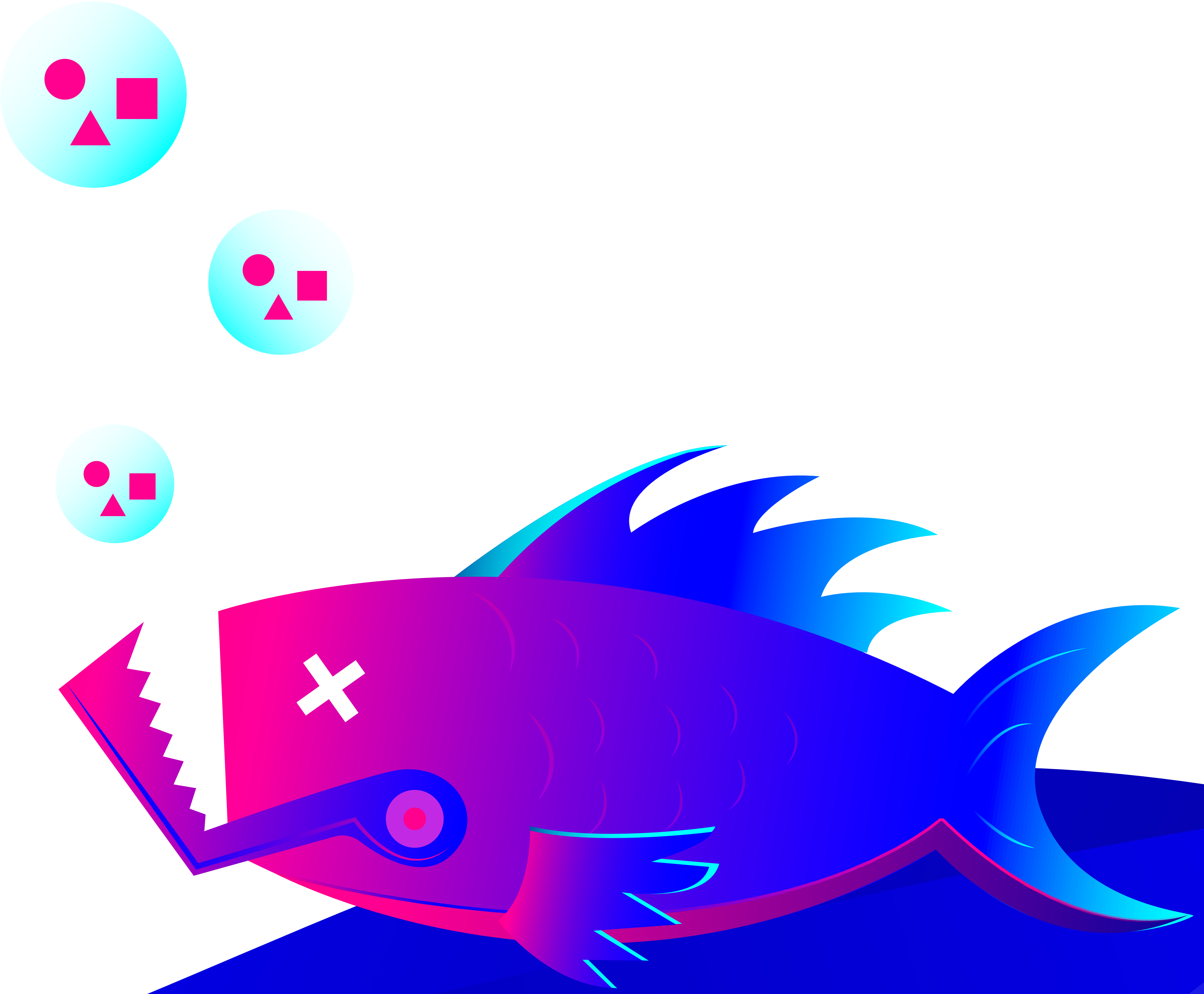
Option: deploy ransomware and get paid a ransom

Decide: Who is my victim? And what's the best way of reaching them?



“It’s not the strongest of the species that survive, nor the most intelligent, but the one most responsive to change”

- Charles Darwin



Just like in nature, when it comes to phishing the key is to be responsive. The attackers are constantly customizing their attacks. As a result of this fast-paced evolution cycle, phishing attacks today are much more advanced than those of only a year ago. And the pace of their development is accelerating all the time.

What Do Attackers Want?

What do the hunters look for when attacking an individual or organization? What is their goal? Is it credentials, sensitive information, a wire transfer to their account?

Credentials

Harvesting user credentials by impersonating, for example, an Office 365 login page.

This allows attackers to access almost any part of the organization, send emails as an employee, and quietly exfiltrate data.

Cash

Either target the CEO and harvest their credentials, or just pretend to be sent from their email address.

Email the CFO for example and demand an urgent transfer of cash to an offshore account.

Data

Attackers can steal confidential information, intellectual property (IP), or customer data.

Attackers can also leverage this information – threatening to sell it on the dark web – and demand a ransom payment.

Sensitive Information

Compromise an email account in the organization and place a silent rule that forwards all incoming emails to the attacker – providing a continuous flow of valuable information that can be used in a mega attack.

The Hunt

Now that they have their end-goal in mind, how does an attacker pick and approach their victim? There are 4 broad categories of prey:

Individuals

- All victims have banking, credit card or PayPal accounts which can be stolen.
- Everyone has an email address, and anyone can send them an email.
- Level of protection and awareness is low.
- Can use compromised accounts to reach victims' connections.

Small Organizations

- Lack effective defenses.
- Attackers can spread to customers, suppliers, partners and employees (e.g. help the attacker penetrate employees' accounts and steal their credit card details).
- More likely to pay a ransom - a malware attack can destroy a small business.

Large Organizations

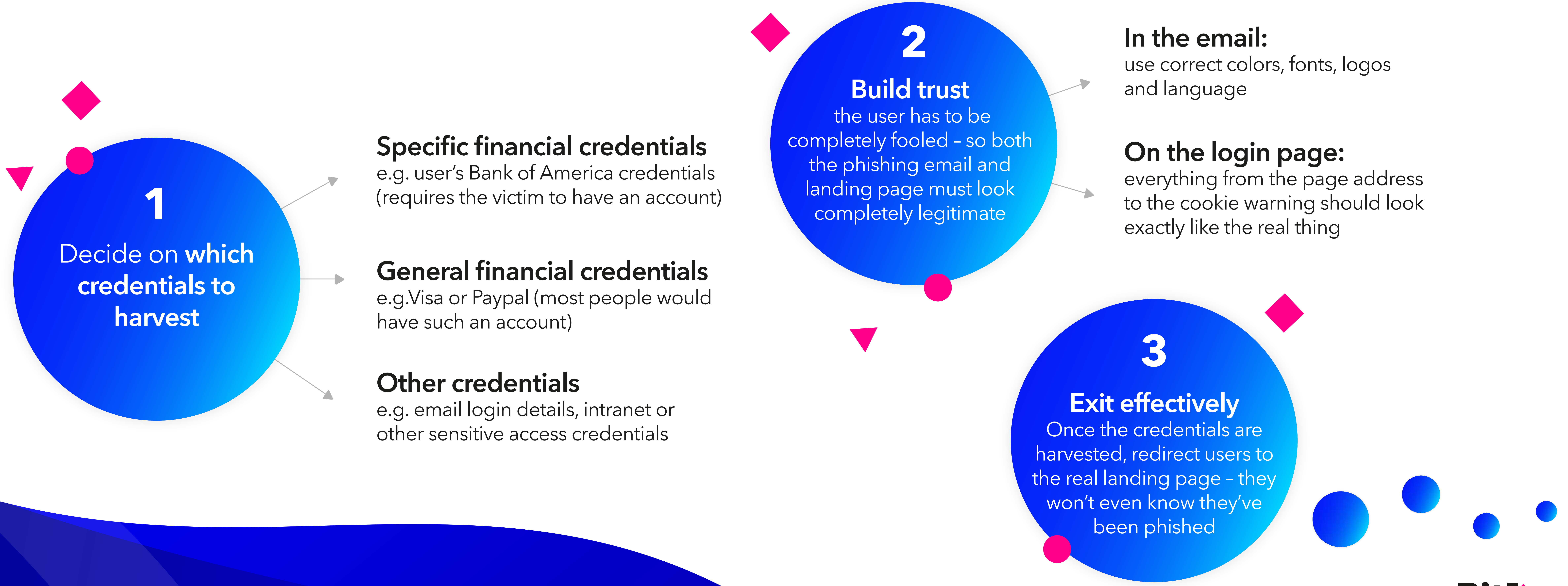
- Compromising a well-known brand allows scaling of the attack.
- Can spread to customers, suppliers, partners and employees.
- Somewhat effective defenses but large surface area makes it difficult to protect whole organization effectively.

Government

- Usually well protected with smaller number of employees than a large organization.
- Often regulated, which makes their security stronger.
- Attacks need to be highly targeted at specific employees.
- Attacks are well planned and generally highly sophisticated.

Carrying Out The Kill

With both the desired victim and potential reward in mind, the attacker goes in for the kill.
How? Let's say the attacker wants to harvest user credentials:



1

Decide on **which credentials to harvest**

Specific financial credentials
e.g. user's Bank of America credentials (requires the victim to have an account)

General financial credentials
e.g.Visa or Paypal (most people would have such an account)

Other credentials
e.g. email login details, intranet or other sensitive access credentials

2

Build trust
the user has to be completely fooled – so both the phishing email and landing page must look completely legitimate

In the email:
use correct colors, fonts, logos and language

On the login page:
everything from the page address to the cookie warning should look exactly like the real thing

3

Exit effectively
Once the credentials are harvested, redirect users to the real landing page – they won't even know they've been phished

Details Matter

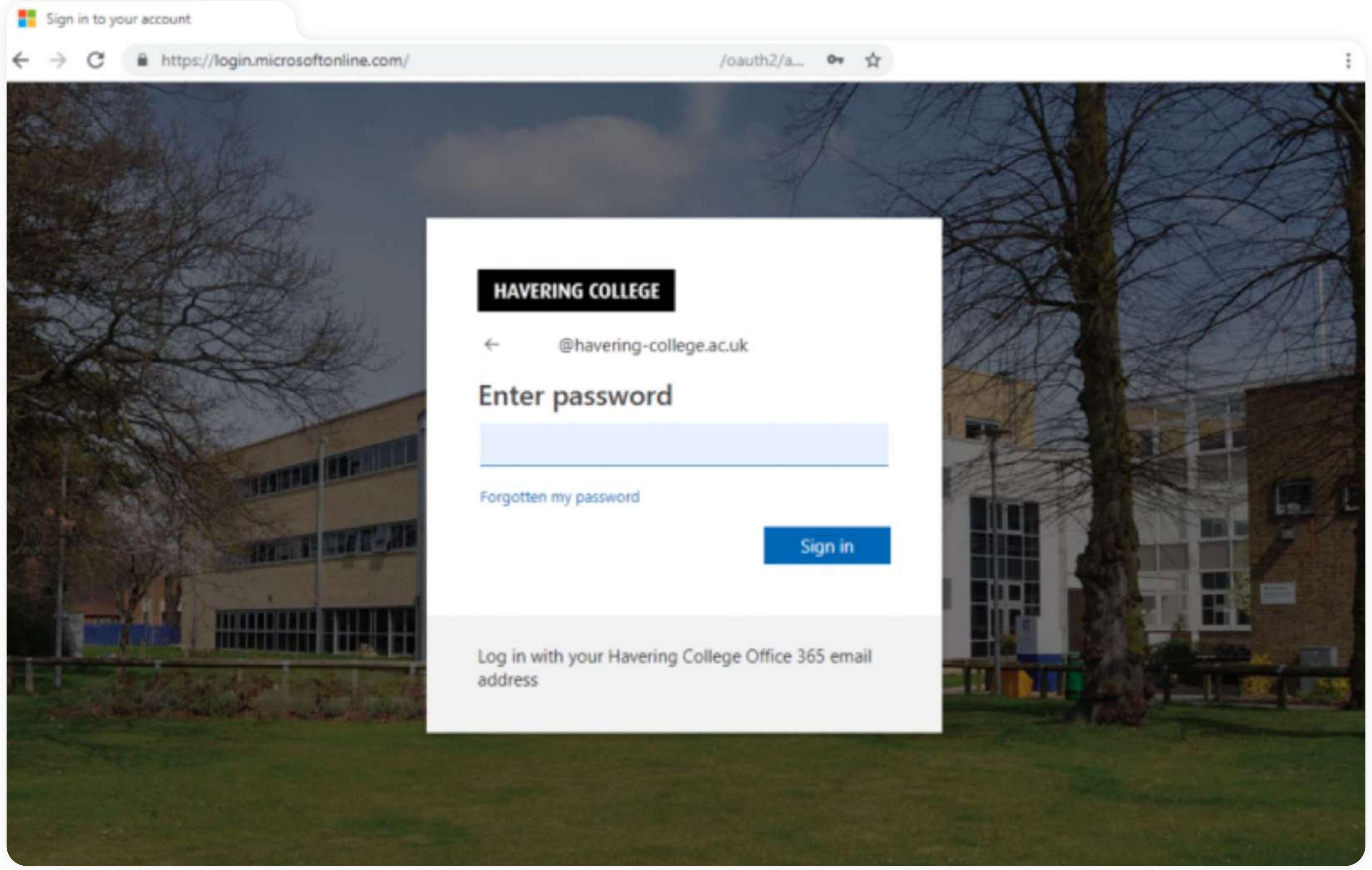
As phishing attacks become more sophisticated and the use of automation in phishing kits becomes more common, phishing attacks are looking increasingly real – and almost undetectable to the naked eye.

For instance, we recently came across a new trend, where attackers create a tailored O365 login page, complete with logo and background that is dynamically changed based on the domain of the attacked email address.

If organization "A" is attacked, users would see a login page with their own organization's logo – dramatically increasing the attack's effectiveness. Read more about it.

Every detail counts.

The URL should mimic the real thing as closely as possible ("paypal-payment-gateway.com", for example, is completely unrelated to the real company) and of course the fake login page should be secured with https.



Log in with your Havering College Office 365 email address

Example: Fake tailored O365 login page

BitDam

Details Matter

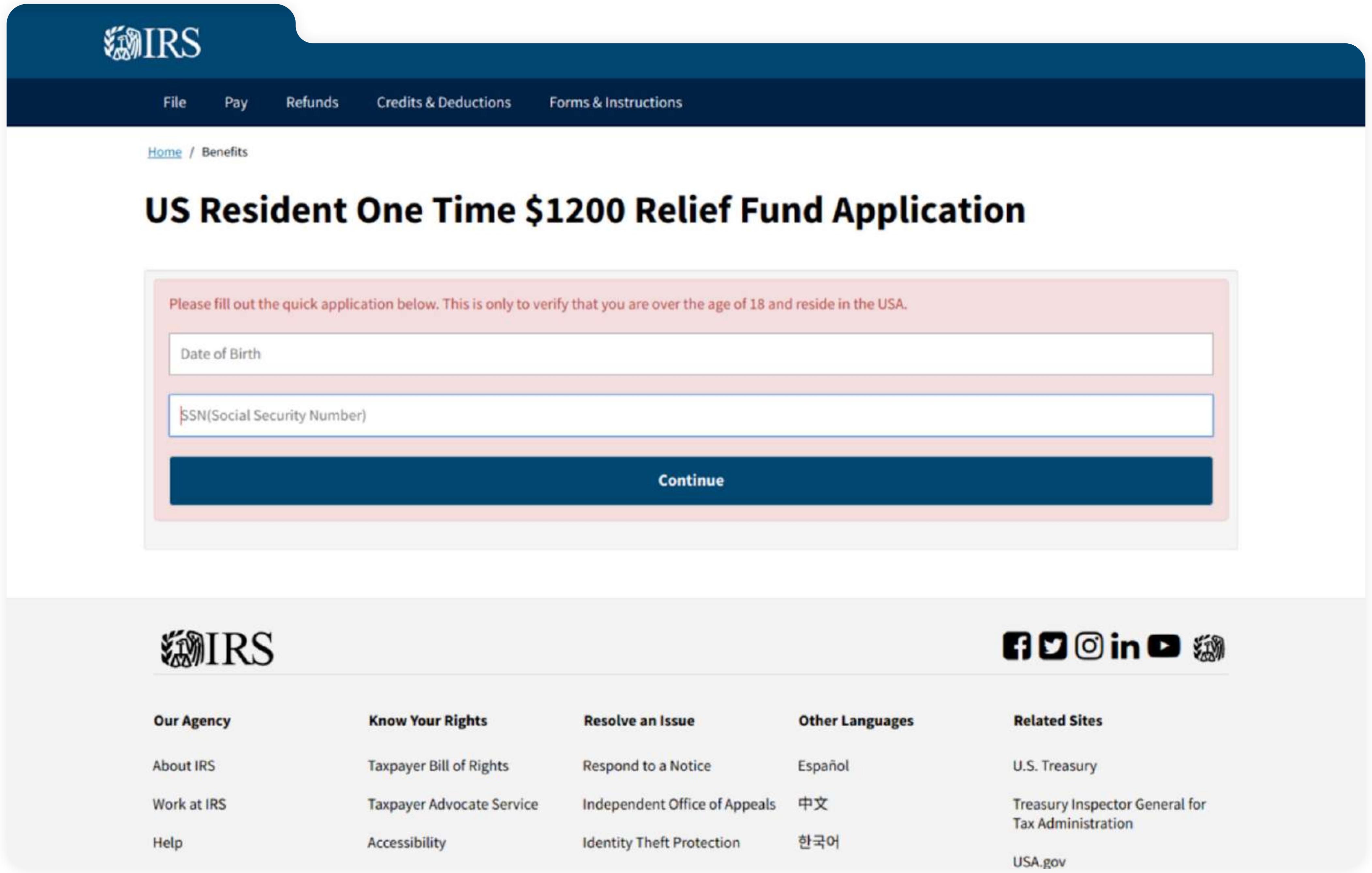
Urgency is key.

Attackers will leverage this to convince the user to take an action, such as entering their credentials. Messages such as “Urgent: Your Emails Are Not Being Delivered” are not uncommon.

From an attacker’s perspective, consistency and matching are critical. So if an email refers to an IRS refund, the landing page would have to mimic a real IRS page.

Attacks are more successful when related to news and current events – a recent example being the $1,200 Covid-19 stimulus check, and another one being related to voter registration.

The bottom line? Just like with so many things, packaging and presentation are everything when it comes to phishing emails. This factor is a key differentiator between successful and failed phishing attacks.



US Resident One Time $1200 Relief Fund Application

Please fill out the quick application below. This is only to verify that you are over the age of 18 and reside in the USA.

Date of Birth

SSN(Social Security Number)

Example: Fake IRS webpage

The Attacker - Defender Relationship

As an attacker, how can I bypass detection?

Why is a really good fake a really bad idea?

How are phishing attacks set up technically?

How can I minimize my chances of getting caught?

Mind Games

Practically and technically, where do attackers start when crafting a phishing campaign?

Hosting

Step 1 is hosting. Hosting is basically the server that hosts the malicious website the attackers serve to the victims. This is the basic infrastructure required to harvest credentials or trick users into divulging confidential and sensitive information. This is where the fake landing page will "live".

Domain names

Step 2 is the domain name: essentially mapping a bunch of letters to an IP address to which the browser will reach out when it tries to retrieve the page in question.

Today, most users will hover over a link before clicking. Thus at first glance, the URL needs to look legitimate, otherwise the potential victim will not continue along the phishing path, and all effort will be wasted.

The Tricks They Play

Attackers will use various ways to hide the true nature of the website in question.

- Redirects to URLs that won't arouse suspicion
- Buying domains that have something in common with legitimate companies; something like "microsoftoffice365online.biz"
- Similarly they can purchase domains of well-known brands and replace an "O" with a zero, or an "L" with a "i"
- Hosting a site with a well-known (and trusted) 3rd-party, such as Google forms, Office forms, Azure storage or Amazon

Also critical is domain reputation: this is key in evading scans and checks by commercial email protection tools.

Finally, attackers are likely to target victims in other countries – thus minimizing the chances of being caught

Subterfuge and Camouflage

Fake it until you make it

Have you ever faked anything? A note from your parents when you were in middle school? An ID to buy alcohol when you were underage? If so, you probably understand why creating the impression of legitimacy is so important.

Deception is the name of the game when it comes to phishing attacks. Every detail has to look real, and all minutiae need to be considered.

You want your fake website or landing page to look exactly like the real thing – so real that your victims would never be able to tell the difference.

Or do you?

But don't fake it too well

Here's where it gets interesting. As an attacker, email protection companies are your nemesis. You have to constantly duck and evade their detection methods in order to reach your end-user victims.

And the email protection companies are on the lookout for legitimate-looking fake websites. So if your "Bank of America" website looks too much like the real thing (and doesn't use the actual BoA website address) they'll be all over you and your phishing attack will fizzle into nothing.

This means that your fake website has to be good, but not too good. It's a delicate balancing act, but one that experienced phishers are able to easily navigate.

Attackers are constantly coming up with new ways of evading email protection companies. One novel way is by using an automated CAPTCHA which would help the attack evade these organizations. You can see more details about this technique here.

Making the Escape

Once credentials are harvested or data copied, the attacker is limited only by their imagination. Thinking big, attackers can:

For individual victims

- Change default shipping addresses for accounts like Amazon or AT&T
- Transfer money offshore
- Buy cryptocurrencies to avoid detection
- Sell stolen credit card data
- Buy online gift cards
- Pilfer tiny amounts from multiple accounts which scales to impressive revenues
- Create dummy apps on Google Play and pay themselves for these apps

For corporate victims

- Harvest Office 365 or G Suite credentials
- Access all internal organizational data
- Re-use the same passwords elsewhere to deepen the phish
- Access 3rd-party tools like Salesforce
- Infect other people in touch with the victim account
- Perpetrate a Business Email Compromise (BEC) attack, otherwise known as "CEO fraud"
- Send fake banking details to customers
- Reply to old email threads
- Change links in internal and knowledge-sharing documents

The Future of Phishing

While email is likely to be the main way attackers deliver phishing attacks for a long time to come, already we've been seeing some changes on the horizon.

Increasingly attackers are leveraging collaboration platforms such as Zoom, Microsoft Teams and Facebook to perpetrate phishing attacks.

As more people work remotely and need to collaborate quickly and effectively, these type of attacks are likely to skyrocket.

If there's one thing we've learned, it's that attackers will use any way possible to dupe users into clicking the wrong link or divulging sensitive information – no matter how unethical, unscrupulous or unfair.

So stay alert, keep evaluating your defensive solutions, deploy a powerful anti-phishing solution that will effectively scan your emails and other collaboration tools, do as much phishing training as possible and if you receive an odd email that you're not sure of – remember everything you've read here.

If you're ever in doubt about an individual phishing email, check it immediately at bitdam.com/is-this-phishing. For a comprehensive solution for your organization, visit bitdam.com/solution.

BitDam

BitDam is a pioneer in cyber defense, securing enterprise email (Office 365, G Suite, Microsoft Exchange), cloud drives (OneDrive, Google Drive, Dropbox, Box, etc.) and other collaboration tools from ransomware, malware, and phishing.

BitDam Advanced Threat Protection (ATP) is proven to detect and stop the > 25% of unknown threats that all others miss. Unlike the alternatives that give a grace period to unknown cyberthreats, BitDam's patented attack-agnostic technology stops malicious files and links at first encounter. Independent of feeds, reputation and intelligence services, BitDam's cloud-based solution detects never-seen-before attacks of any type, providing a remarkably high detection rate and empowering organizations to collaborate safely.

Recognized by Gartner as a 2020 Cool Vendor and by Frost & Sullivan for its technology leadership, BitDam's award-winning ATP solution is utilized by hundreds of thousands of end users and is deployed by leading organizations worldwide, with a proven record of detecting threats that other security solutions fail to uncover.

Try our free tools

- Is this Phishing - online phishing URL scanner
- BitDam's next generation Breach & Attack Simulation - Lucky Meter
- Is this malicious - online malware file scanner
- Free 30-day trial

Learn more about phishing

- BitDam blog
- BitDam webinars and video talks on BrightTalk

To find out more, get in touch at info@bitdam.com.