FORTRA

Brand Threats Masterclass

Experts Reveal Top Attacks and Defense Tactics for 2024

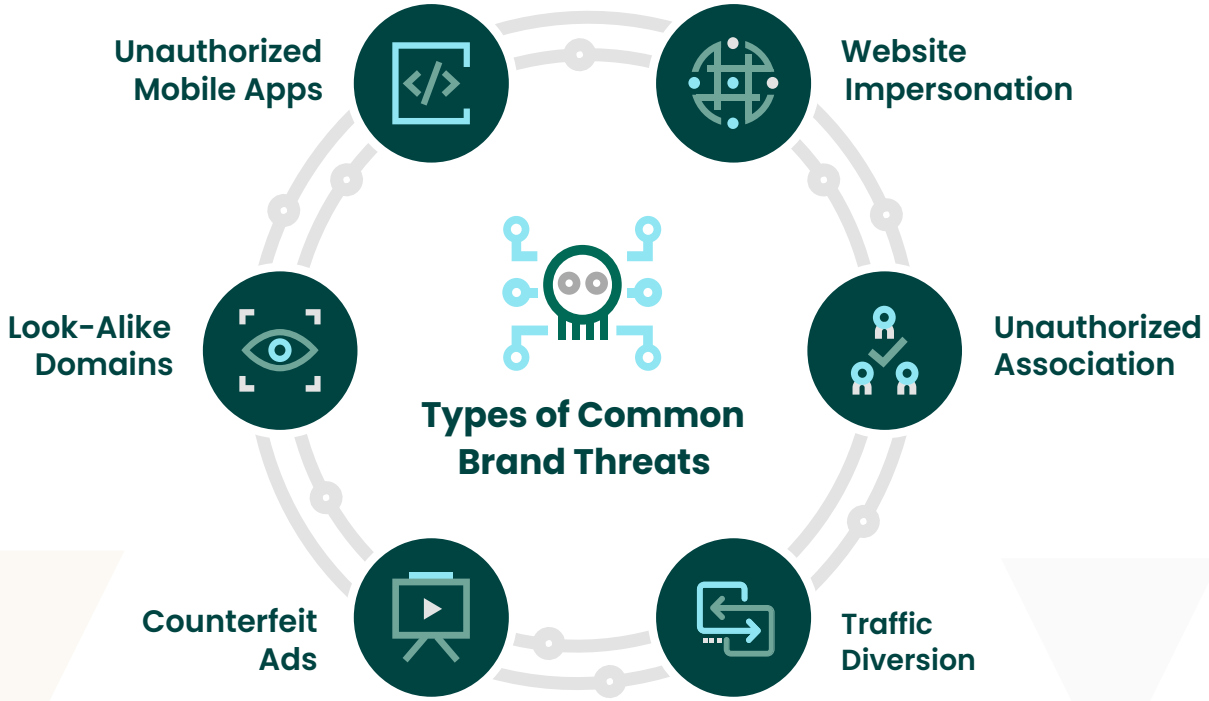
Table of Contents

Brand Threats Masterclass

Experts Reveal Top Attacks and Defense Tactics for 2024

This year, the threats that kept security teams up at night were AI-crafted impersonation campaigns constructed with look-alike domains, customized phish scaled via dark web tools and attacks mimicking brands in hybrid operations across multiple channels. While actors continue to use high-volume attacks as a popular means of targeting organizations, many are diversifying how they initiate fraud, with a growing number of campaigns first touching victims via QR codes, social media ads, and collaboration tools.

Anticipating how brand threats will continue to evolve is challenging due to limited visibility and a lack of understanding into the full scope of the threat landscape. To better inform enterprises of the brand impersonation attacks ranging across the threat ecosystem, Fortra consulted with six of our Digital Risk Protection experts in a recorded roundtable to learn how these attacks manifest and what organizations can do to better protect against them in 2024.



Q+A

The questions presented to our experts below come from industry thought leaders and were designed to generate practical, solution-based responses that security teams can use to better defend their organizations against attacks in 2024.

Each of our experts draw from specialized knowledge in a range of cybersecurity spaces.

THE ROUNDTABLE WAS MODERATED BY:

Michael Tyler

Senior Director, Security Operations

EMAIL SECURITY

Eric George

Director, Solutions Engineering

SOCIAL MEDIA

Omri Benhaim

Security Operations Director, Social Media Threat Intelligence

DARK WEB

Nick Oram

Security Operations Manager, Dark Web and Mobile App Monitoring Services

DOMAINS

Ryan Newby

Senior Security Operations Manager, Domain Monitoring Services

CREDENTIAL THEFT

Tim Farlow

Security Operations Manager, Credential Theft Detection

What have been the most prevalent brand impersonation threats that we've seen, and which ones have been the most impactful?

Brand Impersonation Ecosystem

Cryptocurrency Brand Threats

> **Michael:** Let's start with a general overview of the presence of impersonations in the ecosystem over the past year. **What have been the most prevalent brand impersonation threats that we've seen, and which ones have been the most impactful?**

Ryan: I can kick things off with digital currency and cryptocurrency threats. Several years ago, we were seeing hints of this starting to crop up. Now it's becoming very, very prevalent. And we're noticing they're attacking mobile users more than anything else.

A lot of times these impersonations are targeting financial industries, big banks, credit unions, that kind of thing. And they're going after the mobile users with QR codes and impersonation, saying, "such and such credit union or financial institution is now offering digital currency investments. Please scan QR code, access this credential link, etc.," to bring in targets of theirs.

> **Michael:** That's interesting you bring that up. I know that over the past year, there's been a lot of news about crypto firms having financial trouble, many of the largest firms are declaring bankruptcy. **Do we feel like there's a connection between that financial difficulty and the rise in digital currency-based threats?**

Ryan: Absolutely. I think it's important for us to understand the volatility of that market, and what it means for its end users. A lot of people who get into cryptocurrency are experienced, but there are also a lot of very desperate people looking for a quick buck, a quick investment, or some way to better their situation very quickly. And they're the ones who are not looking at threats as tactfully. They're the most vulnerable ones getting hit with really bad investments - Fraudulent investments that make no sense whatsoever.

And the real target is not necessarily cryptocurrency, but navigating those end users away from the legitimate brand and instead directing them to a fraudulent business.

In Q3, **more than 41%** of threats on social media were impersonation attacks.

PhishLabs Social Media Protection Solutions

Omri: I can add to this on the social side. So, depending on what's trending at the time, impersonations use things like cryptocurrency, NFTs, and things of that nature to be more effective. What we have seen is that impersonations will use promises of gifts like cryptocurrency to legitimize their pages and scam people on a much more effective level.

If you can use what is trending at the time to contact people and get them to click on links which may go to illegitimate websites, phishing pages, download viruses and things of that sort, you're definitely going to be more effective in your overall scamming capability, plus you're going to infect more computers.

One example we saw was when cryptocurrency was at one of its highest peaks, impersonation pages for well-known cryptocurrency figureheads were being created that claimed to be offering giveaways, because that was big at the time. These were very effective in convincing victims and spreading various things like malware and phishing pages.

What role are deep fakes playing in modern social impersonations?

The Role of Deep Fakes and Data Science

> **Michael:** You're absolutely right. Especially when it comes to making a quick buck. You know, social media always has the hottest trends, and seeing that trend around digital currency could easily cascade over to fraud. Pivoting to a different topic around social, the concept of deep fakes has been heavy in the media for the last year or two. **What role are deep fakes playing in modern social impersonations?**

Omri: That's a great question. We are seeing deep fakes becoming more sophisticated and realistic. In fact, if you've been following Instagram recently, there are now what I would call legitimate deep fakes with celebrities where they sign off on their own fake accounts. AI is used to create these chatbots that are exact copies of celebrities. You can have full conversations with them. They will respond to you as real people. It all seems very real.

Scammers use this to their advantage by taking legitimate figures in the celebrity space and creating these deep fake videos promoting various types of cryptos, links and things like that. It's easy to create an account and put up a picture and say, "this is so and so celebrity and I'm promoting this or go do that." But that is a lot less legitimate than somebody watching a video of that person speaking to the camera and telling them "go here, you should do this, you should buy this, you should click on that."

And it's getting to a point now that it's not going to be just prerecorded deep fake videos that they're using, but actual AI chatbots where they're having conversations with the people that they are trying to scam. And you can imagine how deep that can go in terms of what they could get victims to do.

We are hoping to see more technology come out to help identify those types of deep fake videos because it is fairly difficult at this time. And social media platforms in particular are not very good at identifying them. A lot of what has to be done is by people who are trained to identify these things and most people in the general public are not.

> **Michael:** Thanks Omri. Eric, what other types of novel tactics have we seen adversaries incorporating into their impersonations over the last year?

Eric: Well, we have deep fakes as Omri indicated for both scams as well as misinformation campaigns. I think we're also going to see advanced data science applied to the lure side of the attack more than the executable. And for two reasons, really. It's no secret that we as average consumers have some level of personal data that's exposed on the internet, whether it's credentials we put into a platform that become compromised or data we put on social profiles. Also, the fact that we've all seen generative AI applications such as Chat GPT easily produce grammatically correct text on demand.

So, by combining readily available personal data to attackers along with the ability to make believable text on demand, gone are the days you have an "inheritance from a distant prince" type of scam, and enter the days of personalized lures that are going to be much more effective overall.

... another trend that we've seen targeting the enterprise space over the last year has been a growth in hybrid channel attacks.

Can you tell us a little bit more about why those are so dangerous?

Multi-Channel Threat Campaigns

> **Michael:** You know, Eric, as you talk about the evolution of lures, another trend that we've seen targeting the enterprise space over the last year has been a growth in hybrid channel attacks. **Can you tell us a little bit more about why those are so dangerous?**

Eric: We've already spoken to one that's much more prevalent in the last few months - QR codes that are associated with mobile. Now email lures with QR codes are coming in. It's the bridge between mobile and the traditional email. Playing to the comfortable.

More and more we're also seeing a phone number coming in both in enterprise and consumer email-targeted attacks, whereas traditionally, we've seen lures contain URLs or malicious attachments. That phone number is used to get that direct interaction with the targeted user. Also, they can be much harder to block.

Finally, I know Omri and others here are well-versed with the fact that we're seeing a lot of these traditional attacks distributed via social. That's something we're all looking at daily. So it only makes sense the attackers would move there.

> **Michael:** Absolutely. To expand on that, defenses in the enterprise space tend to skew more towards "just in time" defense. For example, rewrapping URLs so that when you click on the link, the service scans it live before you actually go to your destination. With these hybrid channel attacks, generally, you are breaking out of the corporate environment. With QR codes, you scan that QR code with your phone, but the company is not protecting your phone, which means it's going to be able to sail right past any "just in time" defense that's in play. So, definitely dangerous on multiple levels.

Omri: Yeah. I want to continue what Eric was saying because he really hit it on the head with social media being the starting point for a lot of this. You know, gone are the days where people will go on Google and find these phishy links and click on them and get caught that way. A lot of this starts with social media, and that's because that's where the user base is. The majority of people online are using social media, not just for posting about their friends, but for search optimization. They're going there to research brands, find celebrities, find executives, talk about them, and talk with them. It's really a starting point for scammers to be able to reach a really large open pool of potential victims.

Hybrid vishing, or emails containing a phone number lure, can be monetized **through ID theft**, **credit card fraud**, and **malware implantation**.

2023 BEC Trends, Targets, and Changes in Techniques

How are attackers leveraging domain impersonation to launch attacks?

Leveraging Domain Impersonation to Target Brands

> **Michael:** Ryan, this one's for you. So in in the first half of 2023, the average brand was targeted by 40 look-alike domains. So look-alike domains are clearly a huge part of, impersonations. **How are attackers leveraging domain impersonation to launch attacks?**

Ryan: That's a good question. It first starts with the syntax of the URL and a lot of times in conjunction with the top-level domain that it's paired with. We'll get to that in a second.

Often, threat actors will attempt to impersonate a brand by using direct or indirect hits on the brand's title, the brand's syntax itself, the way it's spelled, that kind of thing. A lot of times this also includes pairings with industry-related terms to try and make the URL syntax appear more convincing. If we focus on the finance sector, for example, brands can expect to see terms paired with their brand terms to create a more convincing threat such as finance, invest, portfolio, stock, etc. If I were the owner and operator of ryannewbiescreditunion.com, I would expect to see ryannewbiescreditunion.bank.

And don't forget about top-level domains. They're also being used in conjunctions with the syntax. .ZIP is a great one. You'll have a malicious domain registration paired with a social media comment that points you to .ZIP and then suddenly you're downloading a file. That file could be malware that's now blasted on your organization's network or device.

You need to look at SSL too. A lot of the time people think that an SSL certificate means that it's safe to interact with them. All SSL is saying though is that the person who registered ryannewbiescreditunion.com, for example, is in fact the owner of the site. Anyone can do that. I can register a malicious domain and get it SSL certified because technically, the SSL certificate says that I am the malicious domain owner.

In H1 of 2023, the average brand was targeted by **40 look-alike domains.**

PhishLabs 2023 Domain Impersonation Report

TECHNIQUES TO CREATE LOOK-ALIKE DOMAIN NAMES	
TLD swap:	phishlabs.tech
Subdomains:	phish.labs.com
Typosquatting:	phishlavs.com
Hyphenation:	phish-labs.com
Repetition:	phishllabs.com
Replacement:	ph1shlabs.com
Omission:	phshlabs.com
Transposition:	phsihlabs.com
Insertion:	phishxlabs.com
Homoglyph:	phish.laƄs.com
Vowel-swap:	phishlebs.com
Addition:	phishlabss.com

> **Michael:** Two immediate thoughts based on what you just said, Ryan. First, I'll go on record saying I don't know who thought that .ZIP as a TLD was a good idea, because it's not. The second is that the SSL comments remind me about when, a long time ago, Fortra's PhishLabs put out a shirt that had a green lock icon saying "Misunderstood" because of exactly what you're talking about.

Ryan: Haha, I like that.

> **Michael:** It's so commonly misinterpreted. **So, a follow-up question - Do all impersonation attacks involve look-like domains?**

Ryan: No. They sure don't. A lot of times our teams will see a generic URL that redirects or is blocked through IP/geolocation for specific people in a region. So a lot of the time, it could be a generic URL but when touched on, you're getting navigated to a completely different URL that is actually hosting a threat. You could click on 123.com and all of a sudden, you're being pushed to "Ryan's Faulty Credit Union." A lot of people think that when they click on their primary URL, that is in fact the destination that they're going to, they don't take a look at the browser, their actual landing destination. And that's kind of scary.

Other times, threats can be hidden behind generic URL warning pages. There are also authentication tests. A lot of this has been put in place to circumvent any kind of automated detection that digital risk protection services employ. And the entire purpose of this isn't necessarily to be hidden forever so to speak, it's to keep the domain up as long as possible. The longer the domain is up, the more people it attacks, the older it is, the harder it is to detect, so on and so forth. A lot of it is really to age the domain one day, two days, three months, a year, and then throw the threat up later on down the road.

Index pages are also a thing, in addition to compromising the primary domain. There are tons of different ways to impersonate a brand or confuse people as to what they're looking at.

What makes impersonations in the retail industry unique compared to the sectors that traditionally get targeted such as your tech or your financial sectors?

Brand Impersonation in the Retail Sector

Michael: Let's pivot over to a growing sector where we're seeing more impersonations: retail. **Ryan, can you tell us a little bit about what makes impersonations in the retail industry unique compared to the sectors that traditionally get targeted such as your tech or your financial sectors?**

Ryan: Absolutely. This is definitely an emerging threat space that we've been tracking. One of the things that first comes to mind when talking about retail is counterfeit. Just a major, major problem when it comes to retail brands, clients, products, etc.

We see a lot of counterfeit threats targeting marketplace sites specifically, which have their own set of complications when attempting to take them down. Many of these sites are hosted in regions that are inaccessible to takedowns, such as APAC regions, or hosting providers that are non-compliant, that kind of thing.

Another interesting thing is that they are not really focused on stealing your credentials. They're going for the money. And people are losing money not just indirectly, but directly. Also, with a lot of these sites, you'll actually get a product, believe it or not. It may be completely unrelated to the one that you purchased though or, a knockoff.

Michael: Tim, I know you've spent a decent amount of time looking at the counterfeit space as well. **Anything to add there?**

Tim: Yeah. One of the things I wanted to expand on is what the threat actors are doing with these counterfeit sides to make them appear more legitimate, for example setting up entire login portals. They also incorporate legitimate payment services like PayPal. Like Ryan mentioned, the goal is to steal money, not to steal credentials, and those login portals make these sites more well-rounded and convincing.

Common Types of Counterfeit Activity:

- Fraudulent Advertisements
- Unauthorized Account Pages on Social Media
- Illegitimate Online Storefronts

Michael: How are these counterfeit scams typically being distributed? Is it traditionally through email or are there other vectors that potential victims need to be on the lookout for?

Ryan: So one example is marketplace scams. With that, you're kind of relying on browser-based searches. They're going to try and get their sites as far up as they can on Google.

Michael: Sorry, Ryan, for my clarity, **can you briefly explain what you mean by a marketplace scam?**

Ryan: Absolutely. So, think of a primary site that's trying to draw in end users from a lot of different brands that maybe focus on the same industry. Actors cast this ginormous net, trying to draw in as many people as possible.

For example, I collect and enjoy watches. A lot of marketplaces will host watches that are obviously not from brands such as Rolex, Omega, etc. Same with purses, as well as other fashion items, sunglasses, leather goods, that kind of thing.

That's just marketplace sites. Also, we're seeing browser-based searches used to distribute this type of threat. More often than not, counterfeit items are paired along with social media and social engineering posts. So you'll get somebody who has built up some type of a following on social media and they say, "Hey, I found this really great market site. It's offering discounts on a bunch of Ray Ban sunglasses." And you're going to get that link right through the social media site.

This threat could originate from a Facebook ad. It could be a Google ad. It could redirect off of the Facebook or Google ads. It could be targeting the financial industry and then redirect to something completely different based on the cookies and search criteria that it's recognizing within your device. So it can be very, very refined. But again, a lot of these times we're seeing it come through social media posts and a variety of different platforms.

Also, we talk a lot about retail and products, but you have to expand that. Counterfeit can be defined across a number of different products that you wouldn't normally think about, such as financial investments, fraudulent investments, big-ticket events, all sorts of things.

If you’re an enterprise looking to protect your organization from being impersonated,

what are the most critical social media platforms that you need to be keeping an eye on?

Top Social Media Platforms and Brand Abuse

> **Michael:** Speaking of social media, Omri, pivoting back over to you for another question. If you're an enterprise looking to protect your organization from being impersonated, **what are the most critical social media platforms that you need to be keeping an eye on?**

Omri: Very important. That's actually a two-part question because social media is very complicated in regard to platforms. Some of them are app-based, some have multiple locations where we can access them. Before we answer that question, we have to ask what is actually monitorable on the social media landscape, because we do have to point out that not all of them are. Some of this is based off terms of service, access to APIs, whether it's app-based, or overall restrictions that the platform puts on itself.

Within the monitorable platforms, we really want to focus our attention on the ones that provide the largest pools of potential targets with the weakest impersonation safeguards, the most recognizable legitimate brand names, and of course who the target audience is. So the ones we really want to focus on are the top five: Facebook, Instagram, TikTok, YouTube, and X/Twitter. And really, within those, Facebook, YouTube, and TikTok are the top-used social media platforms globally, with each platform boasting a user count of between 1.7 to 2.9 billion. And that's very important because what they're doing is providing a free and direct path to a never-ending pool of potential targets. Instagram and X/Twitter also provide a large pool, but have dropped in their user count over the last few years.

TikTok is particularly interesting because they have seen an increase in brand usage of about 46% over last year, which is a huge increase. And it continues to grow in popularity, especially among younger users. Gone are the days when everybody's going to Google to do their research. The new generations are using social media to search for the things that they are interested in, including the counterfeit items that Ryan was mentioning.

The average brand is targeted by **65 social media attacks** per month.

PhishLabs Social Media Protection Solutions

X has tried to curve their impersonation issue as you've probably seen in the media recently. They haven't really succeeded at that, and it continues to be an issue. But those five platforms really represent the greatest risk of impact for impersonation across the social media landscape.

> **Michael:** Yeah, I'm seeing that a single social media platform has almost three billion users. That's like 45% of the human population on a single platform.

Omri: Yes. And think of those platforms together. Most people don't use one platform, most use between three to four social media platforms. So there are multiple attack vectors that scammers can use to target their victims. And because social media continues to grow and new users are continually coming on there, it's a never-ending pool.

What role does the dark web or “underground” play in enabling adversaries to launch and monetize brand impersonations?

Brand Impersonation on the Dark Web

> **Michael:** Let's pivot over to the dark web for a minute. **Nick, what role does the dark web or "underground" play in enabling adversaries to launch and monetize brand impersonations?**

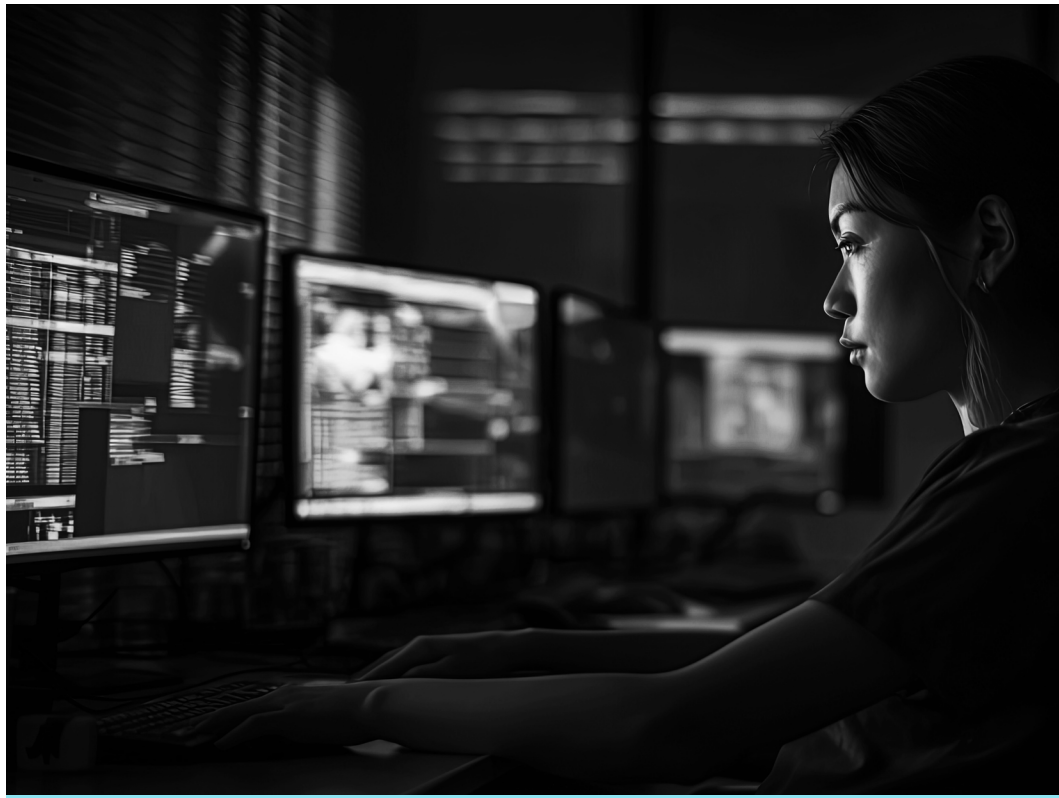
Nick: There are many financial fraud, hacking, leak-based forums out there where fraudsters will advertise their services for free, or where they're looking for potential buyers for their service. I think a common example that you see over the dark web is third-party actors advertising their methods, or guide services to commit various levels of fraud. These threat actors will sell a service for a fee, where you have to reach out to them over a private message on the forum or via an outside chat-based communication channel to pay them for the information. Typically, these guides for their services will contain detailed documents on how to commit fraud.

Forums are a perfect way for individuals to meet like-minded people looking for the same type of thing to exploit. Maybe it's a fraudster looking to find a phish kit, maybe someone looking for a link to do an OpenBullet config tool, database leaks, or carding data. They all meet on these forums to discuss similar topics, exchange services, sell goods, and talk about the fraud they're committing.

> **Michael: Do organizations need to do anything in particular with regard to the dark web when they're trying to build a security posture against impersonations?**

Nick: Yep. I think a lot of people don't really think it's an area where impersonations occur. They just assume they occur on the open web. But it's important to have dark web monitoring protections for your business as well as to protect your customers because lots of activity outside the dark web can result in assets appearing there. Using a password for multiple sites, having your credentials grabbed through an OpenBullet config tool, a phishing email or an infostealer can all lead to stolen credentials or card details being vulnerable on an underground marketplace or forum.

The dark web is a very fast-paced environment. Things can change very rapidly; content can go up and down very quickly. Dark web analysts should always be monitoring the latest and greatest sites out there because threat actors are always evolving new tactics and where they are advertising data, leaving organizations at risk.



Can you tell us a little bit about how brand threats targeting enterprises are different from those that target the consumer space?

Enterprise Email Impersonation and DMARC

Michael: Eric, can you tell us a little bit about how brand threats targeting enterprises are different from those that target the consumer space?

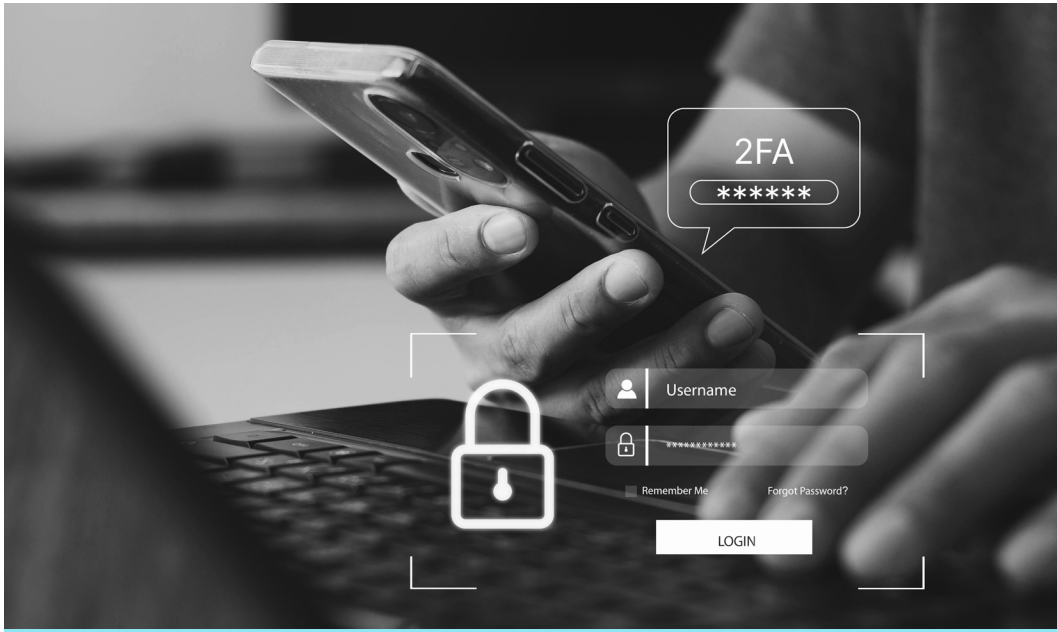
Eric: There are differences for sure. I think you probably know the similarities that we see with these attacks. For example, if we look at them over time, we see that they always leverage well-known brands that the targeted users are familiar with and have some level of comfortability with.

Also, the lures are almost always going to contain an indicator URL. We've mentioned phone numbers a couple of times so far, attachments, things of that nature. And in these cases, actors can create a large volume of attacks and launch them very easily in an automated fashion.

I think the biggest difference between attacks that target enterprises when compared to those targeting consumers would be the overall resources and work that's put in by the actors themselves. With enterprise, there's a lot more of not only researching of the targets, but research of the environment that they're sending into. That's because there are more defenses in place on an enterprise as compared to us everyday consumers.

These attacks are also harder to detect than, generally speaking, the larger commodity attacks that we see. Often, enterprise attacks involve a second stage or an additional action. For example, they not only steal credentials, but may also bring in another stage with an advanced infostealer or ransomware executable.

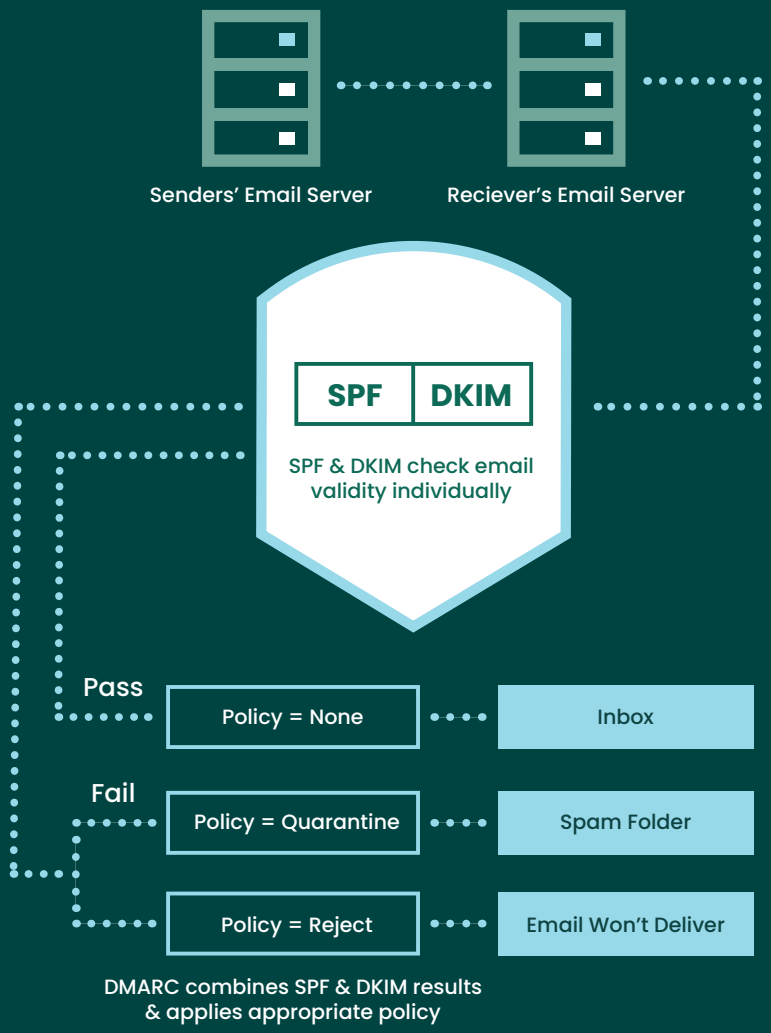
In summary, enterprise-targeted attacks are more complex overall. They're harder to defend against and a single attack can be more damaging. Whereas, while consumer target attacks certainly damaging, that's more like death by a thousand cuts. With enterprise attacks, one email going in can really cause a whole lot of damage that can go on for years to come.



Michael: You know, another area that's been relevant in regards to email security and impersonation is DMARC. DMARC is a major part of email security, it has been for years. Does DMARC stop email spoofing, Eric?

Eric: Unfortunately, it does not. It is however an effective and integral part of combating spoofing of your legitimate domain. And it's even more relevant these days with some of the recent announcements made by some of the biggest receivers in the industry. However, it's not going to outright stop it for a few different reasons.

Number one, it has to be enforced by the receiver of the emails. And we have seen some recent announcements where some of the bigger receivers are going to start looking at the authentication performance and adhering to the instructions put forth in that authentication. However, there are many receivers out there, and not everybody looks at that, and not everybody enforces DMARC. We've seen adoption



gaining over the last five years so we're hoping that trend increases, but that's one place it could fall short.

Another thing is that it needs to be put in place by the sending organization as well. Implemented and implemented correctly.

Enterprises today send thousands of emails, and they usually use a third party to send on their behalf when talking about mass emails. So It's complicated. It takes work. It's a project to get DMARC put in place, and we all have limited resources. So, it might get put on the back burner when it comes to priority, but DMARC has to be implemented by the sending organization.

Finally, it doesn't address look-alike domains. Now while that's not outright spoofing, if I'm an attacker and I go to send something on behalf of Fortra.com, that's what's addressed by DMARC and email authentication. However, if I go and register Fortraa.com with two A's and start sending emails, I actually own the authentication for that. So I could make it look good, and DMARC doesn't address that, it doesn't address the fact that organizations still need to keep a level of visibility onto the look-alike domains target.

In summary, it's effective to some degree. It's like many of the other controls that we use these days. It's not a silver bullet. It's not going to address everything, but something you need to have in place. It's worth the effort for sure.

> **Michael:** There have been some recent announcements around DMARC by some of the major email providers. **How do these announcements affect enterprises and, do they need to do anything?**

Eric: They sure do. The announcements you're talking about here specifically apply to two of the largest receivers and emails in the world, Google and Yahoo. And the announcements apply to mail senders who are sending over five thousand emails a day. Ultimately, for the companies that are sending these emails, it could affect the deliverability of the emails that they're sending out to their customers or their prospects. Those emails could end up getting blocked or quarantined by receiving organizations.

So why are they doing this? Google and Yahoo have both stated that they're doing it to make the email ecosystem healthier. Currently, there are way too many platforms out there that are mail senders, and they can be used by attackers to send malicious emails. So they're looking to make the overall ecosystem healthier by putting these controls in place, and they're really hoping that other large receivers will follow suit. And that's likely to be the case.

So what do companies need to do? There's no shortage of articles on exactly what they need to do to fall in line with the advice and requirements that are being put forth by these senders. First of all, authentication protocols - you need to have SPF, DKIM, DMARC, and make sure everything aligns with your visible "from" senders. So not only having DMARC in place, but you're going to need that alignment with the "from" field.

Also, other criteria need to be in place that are indicative of a healthy sender such as an overall low spam rate and proper unsubscribe practices. For example, if you're sending emails to consumers of that nature, make it easy for them to unsubscribe to those emails. And, you should have some other configurations in there that make it easy to authenticate your mail.

Essentially, Google and Yahoo want to be able to authenticate your mail. And you might look at this as a company and say, "That doesn't necessarily apply to me. I don't send that many emails myself." But you likely work with another third party that does. So making sure that you're in good configuration with that third party to send the emails is going to be essential.

How have attackers changed their tactics when it comes to getting brand impersonations in front of their potential victims?

Trending Attack Techniques

> **Michael:** Tim, tell us a little bit about how attackers have changed their tactics when it comes to getting brand impersonations in front of their potential victims.

Tim: Phishing campaigns being delivered by SMS are definitely not a new thing. However, we have seen a trend of increased volume for this type of delivery, and that's for various reasons.

First of all, SMS platforms do not have the same level of training or conditioning of their users when compared to clicking links on email platforms. Additionally, banking, shopping, social media, and the like are being done more and more on mobile devices, and these devices are almost always on that person. This allows actors to consistently deliver phish to their targets and get them access to malicious links.

Look-alike domains are also used in these scenarios, to both spoof the sender of the SMS message, and to make the URL and the body of the SMS message look legit. With the immediate delivery of these text messages, threat actors are able to capitalize on the sense of urgency portrayed in the campaign, making it more likely for end users to fall prey.

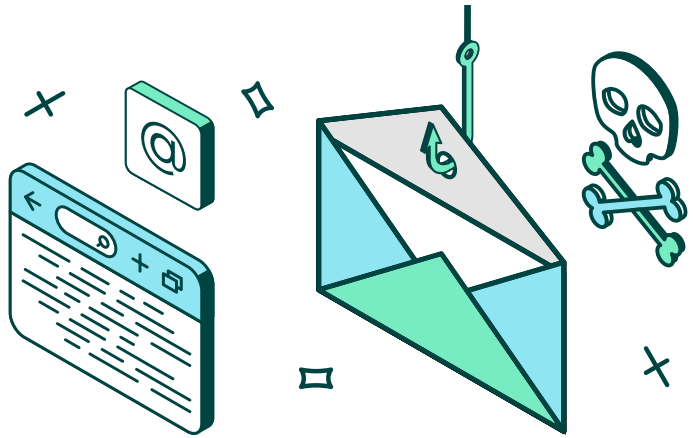
Threat actors can also leverage search engines by spinning up ads that are placed in priority positions in the search results. Look-alike domains add a sense of legitimacy to the ad. A lot of times with these ads, you can see the target of it right below it and you can see the domain in use.

Additionally, threat actors can narrow down the reach of phishing campaigns, which might be weird, but it avoids detection, and allows them to target very specific geolocation and very specific set of clients and brands, typically credit unions that operate in those locations. Ads are also valuable to these threat actors because they allow them to distribute campaigns without needing an email or phone number distribution list.

> **Michael:** How have the goals of consumer-targeted impersonations changed over the last few years? I know traditionally, it's always been about just getting that username and password. **Is that still mainly what we see or have attackers evolved in what they're after?**

Tim: Yeah. I mean, getting the username and password is still important to the threat actor because that gives them account access, but we have seen more complex phishing sites spin up to gather more information such as name, address, phone number, and more, along with those credentials. It allows the threat actors to have access to the accounts being targeted, and possibly even other accounts as well. It also sets the threat actor up to deliver more personalized attacks to that same target, attacks such as password reset scams, or to steal their identity in general. They can also leverage this additional information about this target to impersonate them and then target friends and family with similar attacks.

They're also targeting different platforms. We mentioned crypto platforms being targeted trying to access either the wallet itself or steal crypto in general. They're also targeting e-commerce platforms, spinning up and selling knock-off goods.



Two-part question here:

What techniques can individuals use to avoid falling for these brand impersonations and, is there anything that end consumers can be doing to help defenders fight back?

Proactive Defense Against Brand Impersonation

Michael: Two-part question here: **What techniques can individuals use to avoid falling for these brand impersonations and, is there anything that end consumers can be doing to help defenders fight back?**

Tim: First off, being able to report the impersonation attack is key for defenders to start the mitigation process, and reporting should be done through the appropriate channels such as the abuse mailbox of the platform being targeted. Many have been trained or conditioned to report junk emails they've found, but that same condition hasn't been really applied to the SMS platform.

The best thing that can be done is educate on how to defend from these attacks, especially the education of those who are not on the internet a lot and are too trusting of it. Fraud relies on the ignorance of others. Knowing these tactics is valuable to both not fall prey and being able to report attacks.

So what are techniques that can be used? Well, always be thoughtful of what personal information you're about to share, especially if a sense of urgency is conveyed in the request. If you receive a request to access one of your accounts, validate personal information and confirm the legitimacy of the sender before responding. It's important to note, as we mentioned earlier, that senders can be spoofed. Don't just assume the link is safe if that sender looks legit. In fact, as much as possible, don't follow that link. Go directly to that site and then conduct whatever business is needed there. It's probably the most reliable way to not fall prey. However, if you have to follow a link, examine the URL and the sender to determine legitimacy first. Also thoroughly check the URL and sender for minor alterations or discrepancies such as mistyped characters or spelling errors.

Sometimes that's difficult, though because in the body of the text or email, they'll use URL shorteners. So once you're loading the link in your browser, verify what the URL is on their browser. Make sure it's legitimate as well, looking for any discrepancies before providing any information.

> **Michael:** Yeah. I don't know that I've ever seen an official email using a URL shortener for what it's worth. So I think that that by itself can be a pretty big red flag.

Tim: Exactly.

> **Michael:** For the rest of the group, for organizations that are looking to protect themselves, what are the key capabilities that need to be invested in?

Ryan: There are a number of different aspects that companies can do to protect themselves. Obviously, digital risk protection services are going to be the forefront of your consideration. You want to make sure that you are monitoring your threats rather than just purchasing them all at the beginning of the year kind of thing. That can end up becoming very, very expensive.

You also want to make sure that you're blocking threats from entering your workspace, your ecosystem. So when you see malicious registrations, you want to block those domains from ever sending any kind of communications to your team in spear phishing attacks.

And then that said, just branching off, you want to make sure that you're monitoring on a consistent basis for any kind of impersonation threats that are targeting your brands or your end users. In this day and age, it's not feasible anymore to be interacting with top-level domain registries upon release and doing sunrise registrations. That's expensive and inefficient, just with how dynamic threat actors are nowadays. It's more beneficial to instead detect, draw in, case, and monitor these threats on a consistent basis so that when they do become a malicious threat, an actual threat, you're able to take them down as efficiently and quickly as possible. That's my two cents.

Eric: Yeah. I think there are a couple of different ways you could look at this when it comes to targeting an enterprise or defending an enterprise against impersonation attacks. We spoke a lot today about the DRP or digital risk angle as far as the misrepresentation of the brand on external locations goes. Look at home, talk to your customer service representatives, look at items that are being reported by your customers. If you don't have a method for your customers to report abuse, set that up right away. Also do some searching for what types of digital risks and impersonation attacks are targeting your industry. That should give you a good place to start.

Once you have those, look at your existing controls and the amount of risk there, do a little bit of a gap analysis. And then from there, when you know the red hot issues that you need to start with, there's a lot of intelligence that can be gleaned from working groups specific to your industry or just general threat groups overall. There are a lot of resources online. For example, with look-alike domains or social media, there are multiple ways that you can look that stuff up and get some level of insight into if your brand's being targeted or not. You're not likely going to get everything, but you'll at least know where to start. And that will give you a good plan of attack.

I think also one thing that you could really do to set yourself up for success and save a lot of heartache in a fire drill situation is just have a plan for when these risks pop up. Have an owner for any mitigation you'd have to do for those. Have a little bit of research in place so this owner can hit the ground running if something does pop up. That way they won't be caught on their back foot.

Omri: I'd love to add something here. On the social landscape, one of the best ways you can protect yourself is really to be present and be active. And it's really up to brands to make sure they have an active presence on these platforms. Because if you do not, you leave that open for someone else to step in and take that place. Creating legitimate pages that are verified and have activity on them is extremely important so we can see the difference between a fake account and a real account. Have those accounts verified and registered as being active with your user base. That way they know where they need to go when they want to have these conversations with you. Make sure that you spread that information across your legitimate websites and your advertising material, and make sure that you are present on those leading platforms because if you're not, you leave it up to someone else to be there for you.

> "Social media platforms have created the most accessible **pool of potential targets**."

Michael: That's great insight. Thank you for sharing.

Ryan: Can I add one more thing there, Michael?

Michael: Absolutely.

Ryan: I think you know the first step that an organization or a brand can also take is educate to people. If you do not have in-house training or education, find it. My example is slightly anecdotal. My wife, she's a hospice nurse, and her industry, her facility right now in particular, is under attack. Everybody is getting ransomware-type emails, social engineering-type emails, stuff from, you know, a director of care saying something urgent. And a lot of the people that work there are obviously in the health care space and do not understand social cyber, domain attacks, or anything like that.

Organizations need to be aware of the people that are in their industry. You know what I mean? And understand that those people may not understand cyber threats and how refined and how absolutely complicated they can be. Find that education for your people, basically.

Michael: Anyone else with last thoughts?

Omri: We already touched on it with the previous question, but I would just reiterate why social media poses a more unique risk in terms of impersonation. And a lot of this comes back to the user base and accessibility. We're talking about over 4.8 billion social media users worldwide representing 60% of the global population. So social media platforms have really created the most accessible pool of potential targets.

Over four hundred thousand new users join social media platforms daily, which provides actors with new targets that are inexperienced and trusting. On top of this, 81% of brands in general use social media for brand awareness and 80% of users use social media for brand research. This makes brands and public-facing figures very effective attack vectors. And, as we mentioned before, we must always remember that when a social media impersonation page is created, you can also add various other attack vectors to that page, such as malicious domains, links to fake mobile apps, viruses, etc. From my perspective, social media is really the trunk of the tree, with the potential to grow many branches leading to expanded scamming potential.

Final Thoughts

Michael: So when it comes to organizations caring about impersonations, they really have two different types of impersonation that they need to care about. First, people attempting to breach that organization by impersonating a third party, whether that be your mail or email vendor or, some other third party that you do business with. The implications of failing to protect against that are fairly straightforward: account breach, ransomware deployment, potential regulatory issues, loss of trust. You can look at dozens of big news media stories about major brands suffering data breaches and depending on which source you look at, anywhere from 70% to 95% of breaches start with a phishing attack, and of course a phishing attack is just a type of impersonation.

The other side of that coin is how does an organization protect against their brand being impersonated to third parties, whether that be consumers or other organizations. On the face of it, you think, "Well, of course, we should protect our brand." But if you think about it a little bit more empirically, you go "Well, what's the real damage?"

There is real damage to not successfully managing your digital risks. To drive my point home, SAS is an AI and analytics company that specifically works with financials for anti-money laundering and tracking to detect fraud payments. They recently did a consumer survey that revealed two-thirds of consumers will switch brands if they are affected by fraud related to a particular brand, regardless of whether they perceive that brand to be at fault. So, basically saying "I know it's not your fault, that a bad guy impersonated you and stole all of my money, but I'm still I'm still taking my business elsewhere."

Two thirds.

So there's real damage there. And organizations need to keep an eye on what their digital risk looks like, because these scams are only going to continue to grow.

Forta's Digital Risk Protection

Successful Digital Risk Protection requires a comprehensive mitigation strategy that can rapidly and completely protect against online threats. Partial mitigation strategies, such as integrating threat indicators into internal security controls, are not enough to prevent harm to brands, customers, and employees.

Fortra's Digital Risk Protection services safeguard organizations' critical digital assets through expert-curated threat intelligence and complete mitigation against brand impersonation, data leakage, social media threats, account takeover, and other digital risks in one complete solution.

For more information check out **Fortra's Digital Risk Protection Solutions.**

Fortra's Advanced Email Security

Fortra's Advanced Email Security solution delivers comprehensive threat protection and powerful policy enforcement for cloud, on-prem, and hybrid environments by tackling the toughest email security challenges including **business email compromise** (BEC), advanced threats, and **data leaks.**

Fortra's DMARC Protection is an essential email authentication protocol that enables administrators to prevent hackers from hijacking your domains for email spoofing, executive impersonation, and spear phishing.

For more information check out **Fortra's Advanced Email Security Solutions.**

Fortra's Digital Risk Protection Experts

Michael Tyler

Senior Director, Security Operations

Michael Tyler is the Senior Director of Security Operations for Fortra's PhishLabs. He is responsible for supervising the detection and prevention of numerous external daily threats, including phishing, brand abuse, and account takeover attacks. With over 15 years of experience in cybersecurity, Mr. Tyler possesses expertise in social engineering psychology and cybercrime tactics.

Eric George

Director, Solutions Engineering

Eric began his PhishLabs career as an analyst in the Security Operations Center.

He advanced to multiple lead roles while specializing in detecting, analyzing, and mitigating account takeover attacks. After transitioning to Solutions Engineer, Eric was promoted to his current position, leading solution engineering, targeted intel, and technical client support for Fortra's Digital Risk Protection solutions. Since 2021, Eric's team has expanded its scope to include Fortra's Advanced Email Security solutions.

Eric has held over ten industry certifications, including CISSP, and is a Technical Malware Co-Chair for the Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG). He is currently completing a Master of Science degree in Information Security and Cyber Leadership.

Omri Benhaim

Security Operations Director, Social Media Threat Intelligence

Omri began his career at BrandProtect as an analyst in the Security Operations Center. In 2018, he was promoted to Data Manager Specialist when PhishLabs acquired BrandProtect. He then held multiple lead roles, specializing in domains, open web, and mobile. With over 14 years of experience, Omri has developed expertise in social media, cybersecurity protection, brand protection, and online impersonation. Additionally, Omri runs Fortra's cross-functional Subject Matter Expert (SME) program, helping to improve overall operations and service delivery.

Ryan Newby

Senior Security Operations Manager, Domain Monitoring Services

Ryan has been with Fortra's PhishLabs for four years and is currently the Senior Security Operations Manager for domain monitoring services. He leads a team that provides specialized curation and expert mitigation services for superior domain threat fidelity.

Nick Oram

Security Operations Manager, Dark Web and Mobile App Monitoring Services

Nick started his career as a cyber threat analyst at BrandProtect, where he played a crucial role in developing Fortra's current dark web monitoring solution. He has been instrumental in expanding the solution since its inception and was promoted to team lead for the dark web monitoring solution in 2018. In 2021, he moved to his current position as Security Operations Manager. Nick holds a master's degree in Applied Intelligence from Mercyhurst University and has worked in the industry since 2016.

Tim Farlow

Security Operations Manager, Credential Theft Detection

Tim Farlow studied Network Engineering at Purdue University, where he began his career in the DRP industry as an analyst for Outseer's (RSA) Anti-Fraud Command Center. While there, he gained expertise in detecting, analyzing, and mitigating various types of fraudulent content. He was promoted to Team Lead, where he collaborated with other product teams to improve workflows procedurally and technologically. Tim also acted as the primary business relationship contact for several international clients as the Customer Engagement Manager.

Tim became the Operations Manager for PhishLabs' Credential Theft Detection team in 2021, where he enhances threat detection capabilities through technology, automation, and procedural changes. He is currently focused on gaining a deep understanding of the latest techniques used by threat actors to evade detection and finding strategies to overcome them.

FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

(fta-g-1123-r5-am)