TitanHQ PhishTitan

A Phishing Expedition: Why Phishing is The #1 Threat to Your Clients' Security

How MSPs Can Build Comprehensive Phishing Protections for Clients in a Complex Threat Landscape

TitanHQ PhishTitan

Phishy Business: The Current State of Email Security

In 2023, phishing has grown into one of the biggest threats to businesses in the UK. Over are the days where it was easy to identify a phishing email from a legitimate email—cyber criminals have developed increasingly complex methods of impersonating a trusted sender. Today, the UK is the most targeted European country when it comes to phishing.

Over 90% of cyber attacks begin with phishing.[1]

Source: Cisa [1]

96% of businesses in the UK were targeted by phishing in 2022.[2]

Source: IT Governance [2]

74% of all security breaches include a human element.[3]

Source: Verizon [3]

The human element is a prominent factor in phishing attacks, and considering that it takes businesses an average of 277 days[4] to identify a data breach, organizations are often just one wrong click away from potential disaster.

As an MSP, it's more crucial than ever to be able to offer comprehensive phishing protection to your clients. This guide will help you convey the urgency of email security and give you tangible steps you can take to enhance your clients' defenses.

We cover:

- ✓ Modern types of phishing
- ✓ Layers of phishing protection
- ✓ PhishTitan: The phishing prevention tool for Microsoft 365
- ✓ How TitanHQ can help you fortify your defenses

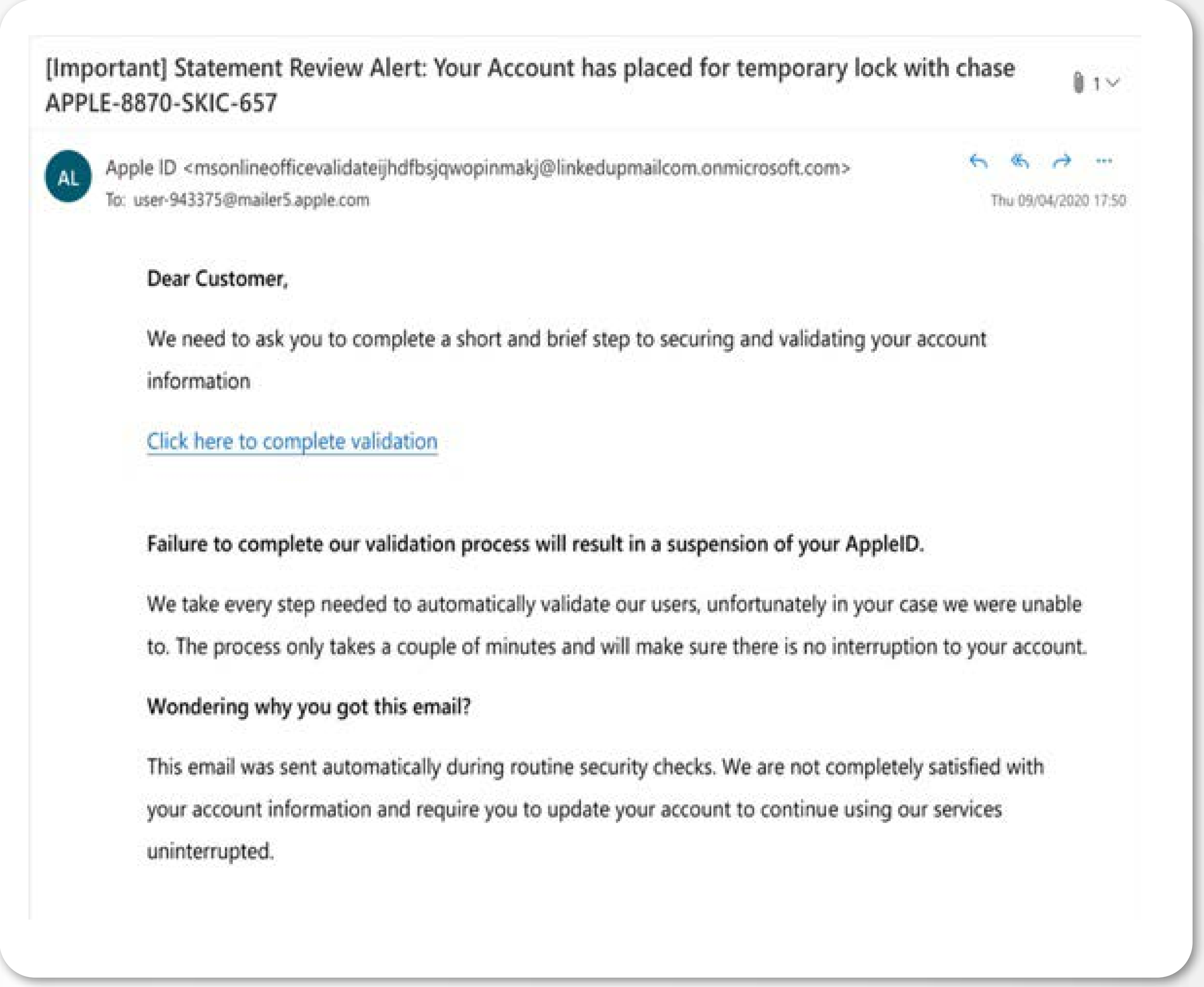
Source: IBM [4]

A Can of Worms: Modern Types of Phishing

While the classic “You have inherited $1 million from an estranged relative” emails are still popular, modern phishing techniques have grown increasingly complex and harder to differentiate from legitimate emails.

Email Phishing

Email phishing attacks are the most common phishing threat that we have all come across both in our private and corporate inboxes. These attacks are not targeted; cyber criminals are figuratively throwing hundreds of hooks in the sea and hoping something bites. The email addresses are acquired by illegal harvesting or from data stolen in security breaches. Often, these emails impersonate a trusted corporation, such as a bank, Apple or Amazon and include a link that, once clicked or downloaded, installs malicious software on the user’s device.



[Important] Statement Review Alert: Your Account has placed for temporary lock with chase APPLE-8870-SKIC-657

Apple ID <msonlineofficevalidateijhdfbsjqwopinmakj@linkedupmailcom.onmicrosoft.com>
To: user-943375@mailer5.apple.com
Thu 09/04/2020 17:50

Dear Customer,

We need to ask you to complete a short and brief step to securing and validating your account information

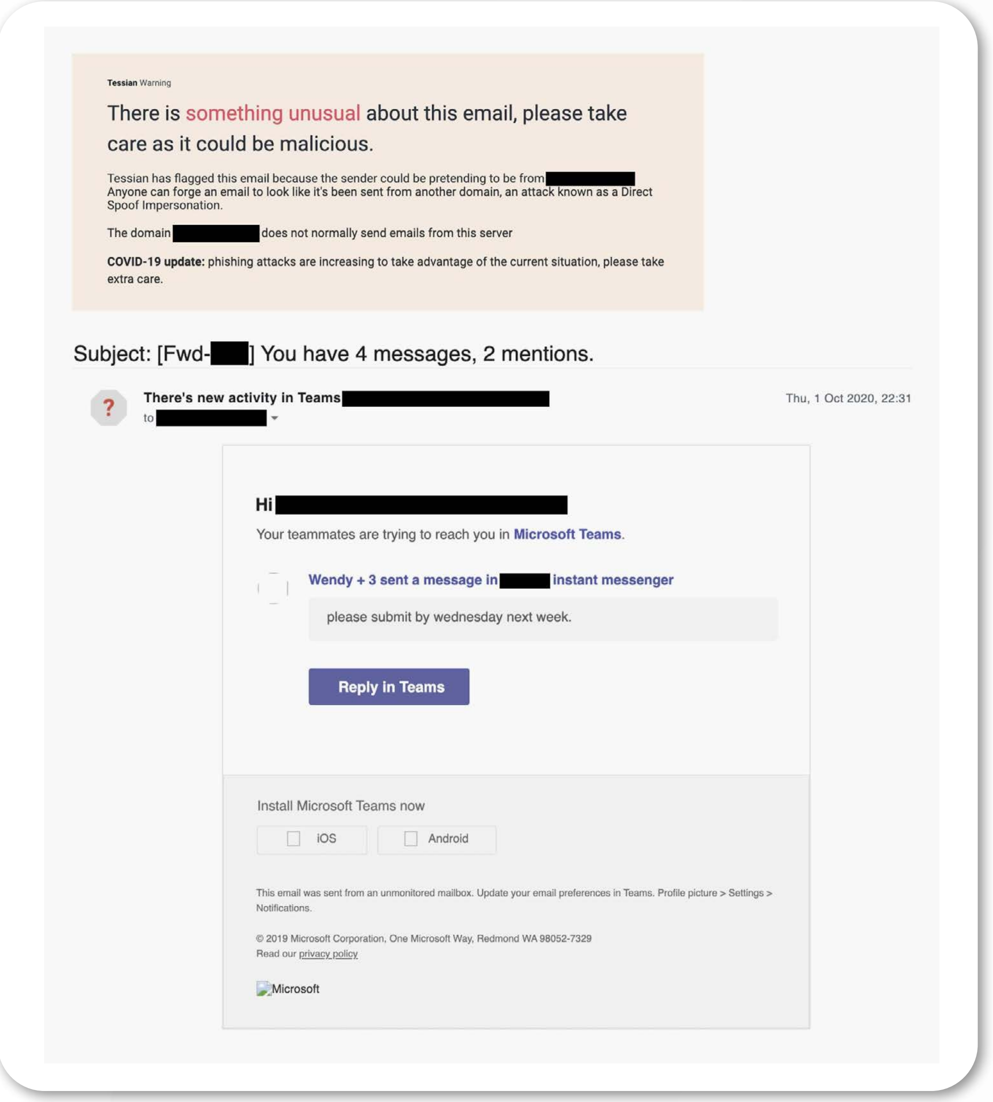
Click here to complete validation

Failure to complete our validation process will result in a suspension of your AppleID.

We take every step needed to automatically validate our users, unfortunately in your case we were unable to. The process only takes a couple of minutes and will make sure there is no interruption to your account.

Wondering why you got this email?

This email was sent automatically during routine security checks. We are not completely satisfied with your account information and require you to update your account to continue using our services uninterrupted.



Tessian Warning

There is something unusual about this email, please take care as it could be malicious.

Tessian has flagged this email because the sender could be pretending to be from [redacted] Anyone can forge an email to look like it's been sent from another domain, an attack known as a Direct Spoof Impersonation.

The domain [redacted] does not normally send emails from this server

COVID-19 update: phishing attacks are increasing to take advantage of the current situation, please take extra care.

Subject: [Fwd-[redacted]] You have 4 messages, 2 mentions.

There's new activity in Teams [redacted]
to [redacted]

Thu, 1 Oct 2020, 22:31

Hi [redacted]

Your teammates are trying to reach you in **Microsoft Teams**.

Wendy + 3 sent a message in [redacted] instant messenger

please submit by wednesday next week.

Install Microsoft Teams now

This email was sent from an unmonitored mailbox. Update your email preferences in Teams. Profile picture > Settings > Notifications.

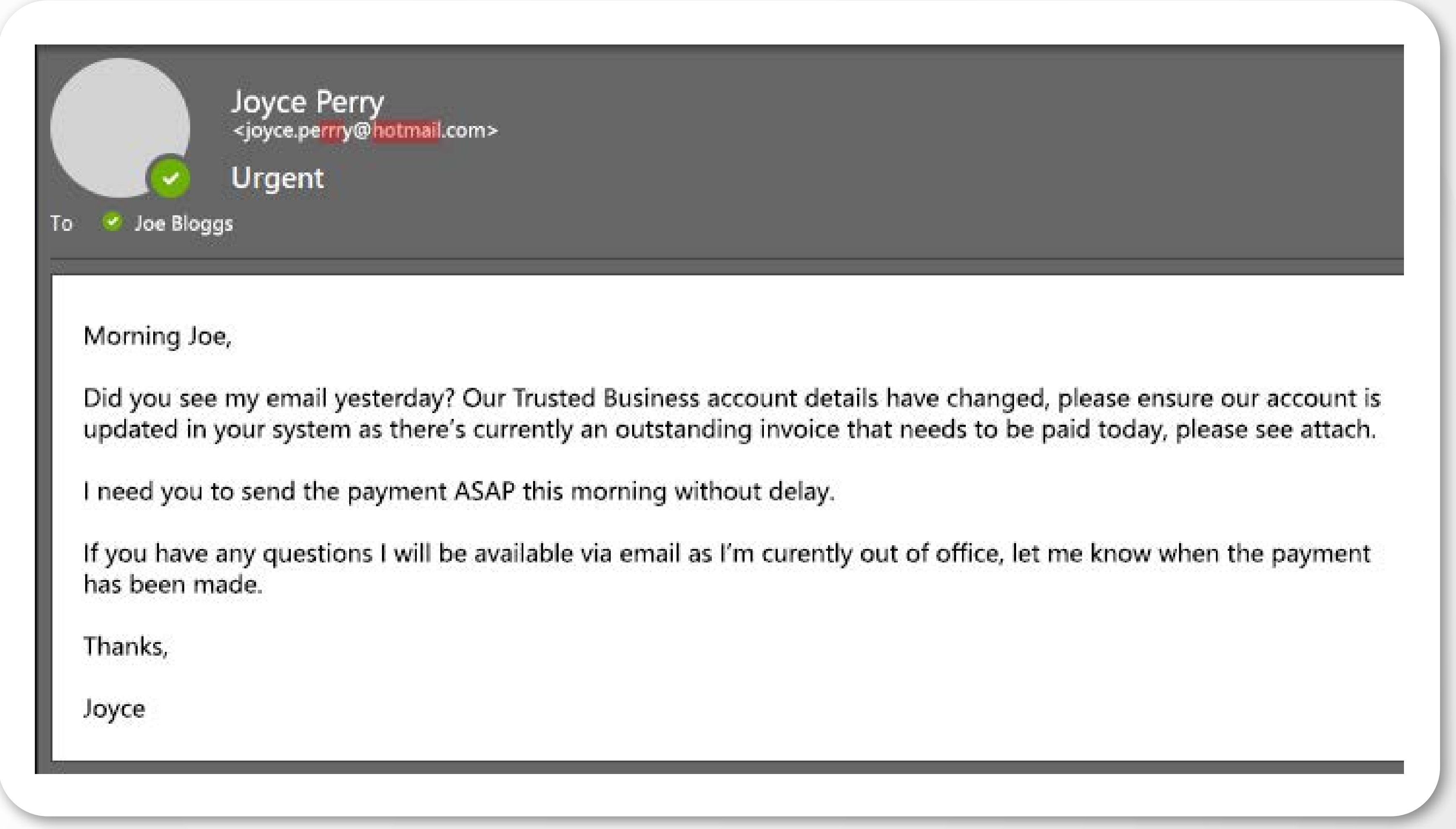
© 2019 Microsoft Corporation, One Microsoft Way, Redmond WA 98052-7329
Read our privacy policy

Spear Phishing

Spear phishing is a more sophisticated version of email phishing. These are better-researched attacks that target individuals in a corporation that have access to sensitive data, such as accountants, system administrators or C-suite executives. The spam mail itself usually is a fake request to download vital business documents or pay outstanding fees and is designed to look like it comes from Microsoft or another trusted application or corporation. Once the recipient follows the link and enters their credentials, the next step in most cases is account takeover by the cyber criminals.

Whaling

Whaling is a phishing tactic that adds an additional layer on top of spear phishing. With this approach, the cyber criminals will specifically target high-profile individuals at an organization, such as C-suite executives or business owners. These attacks are highly researched and use complex social engineering strategies in order to come across as legitimate and deceive their recipients. The whaling emails usually will use extreme tactics (such as threatened lawsuits) to try and trick the recipient into transferring funds or following malicious links.



Joyce Perry
<joyce.perry@hotmail.com>

Urgent

To Joe Bloggs

Morning Joe,

Did you see my email yesterday? Our Trusted Business account details have changed, please ensure our account is updated in your system as there's currently an outstanding invoice that needs to be paid today, please see attach.

I need you to send the payment ASAP this morning without delay.

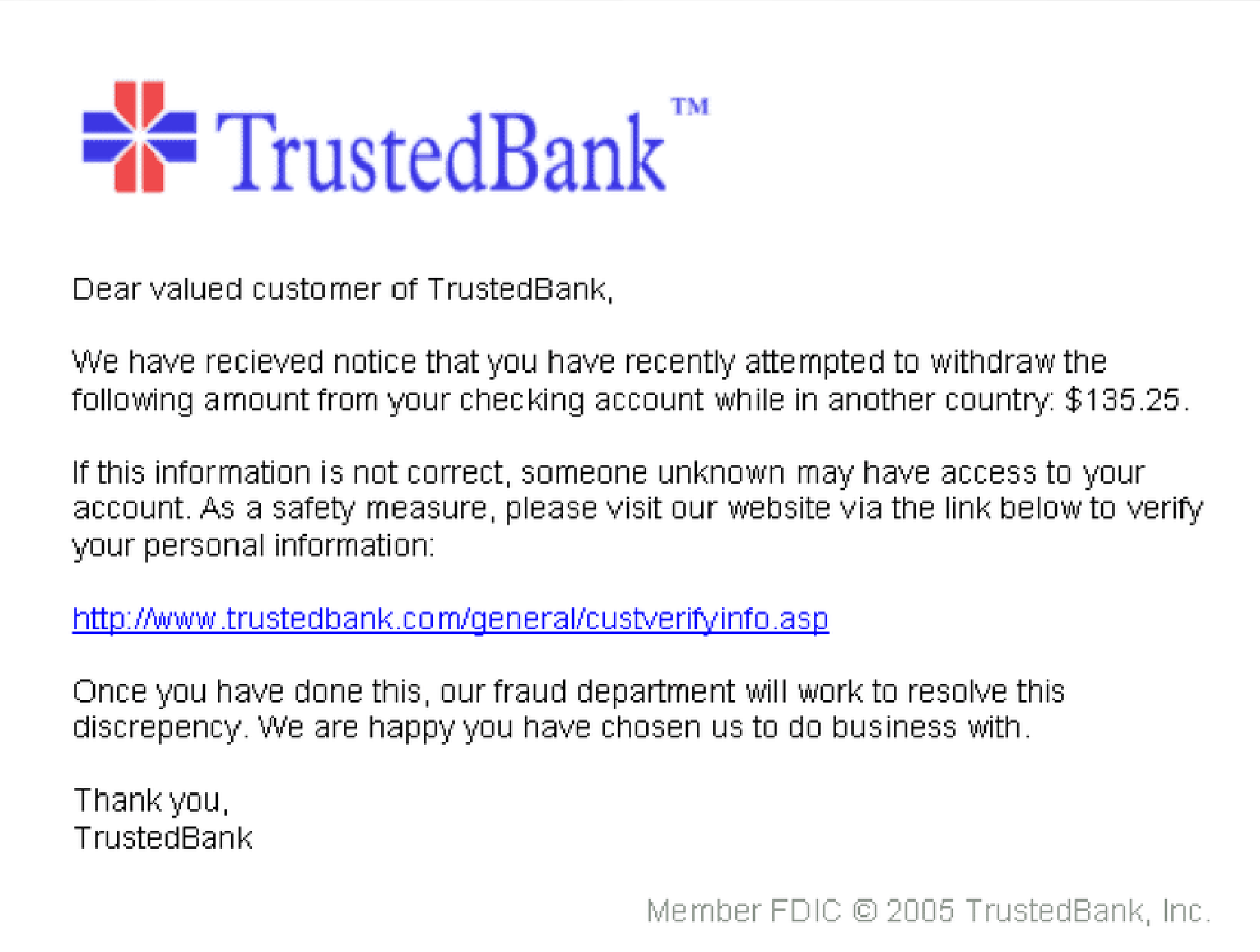
If you have any questions I will be available via email as I'm currently out of office, let me know when the payment has been made.

Thanks,

Joyce

Clone Phishing

Clone Phishing is a close relative to spear phishing. During a clone phishing attack, cyber criminals will clone an existing, legitimate email in order to try and trick the recipients. Think Google verification emails, Apple ID logins or even invitations to webinars or events. Once the criminal has a copy of the original email, they create a cloned copy with the exact wording, branding, and content as the legitimate email, but they will replace the action (I.e., download, register) with a malicious link. This phishing technique is engineered to steal login credentials and other data.



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

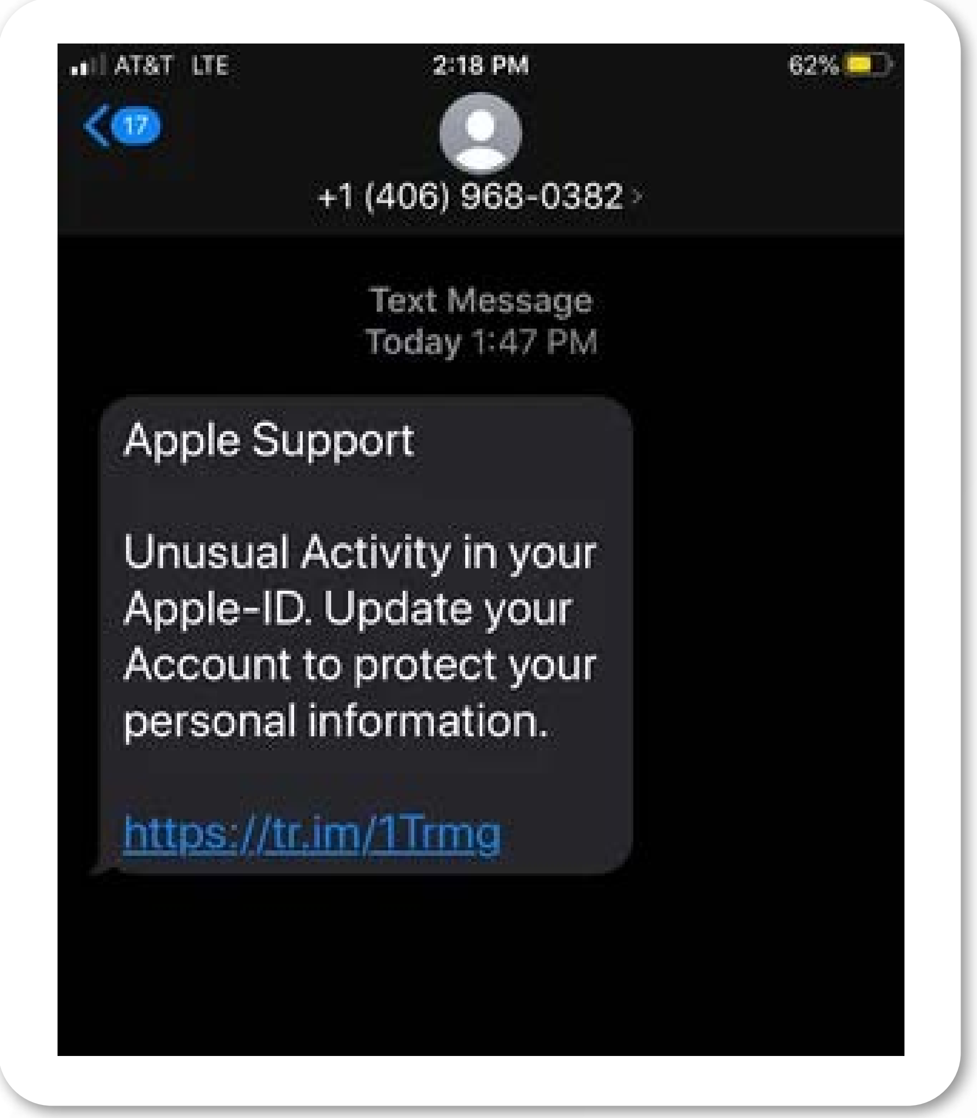
Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Vishing

Vishing is a form of phishing that involves the criminals making fraudulent phone calls (or leaving voice messages) and is often executed in combination with another form of phishing. For example, a cyber criminal will make a phone call impersonating a representative of a reputable company in order to extract sensitive information from the victim, and then follow up with a fraudulent email (such as whaling). Vishing scams are well-researched by the criminals and are usually executed for monetary gain.



+1 (406) 968-0382

Text Message
Today 1:47 PM

Apple Support

Unusual Activity in your Apple-ID. Update your Account to protect your personal information.

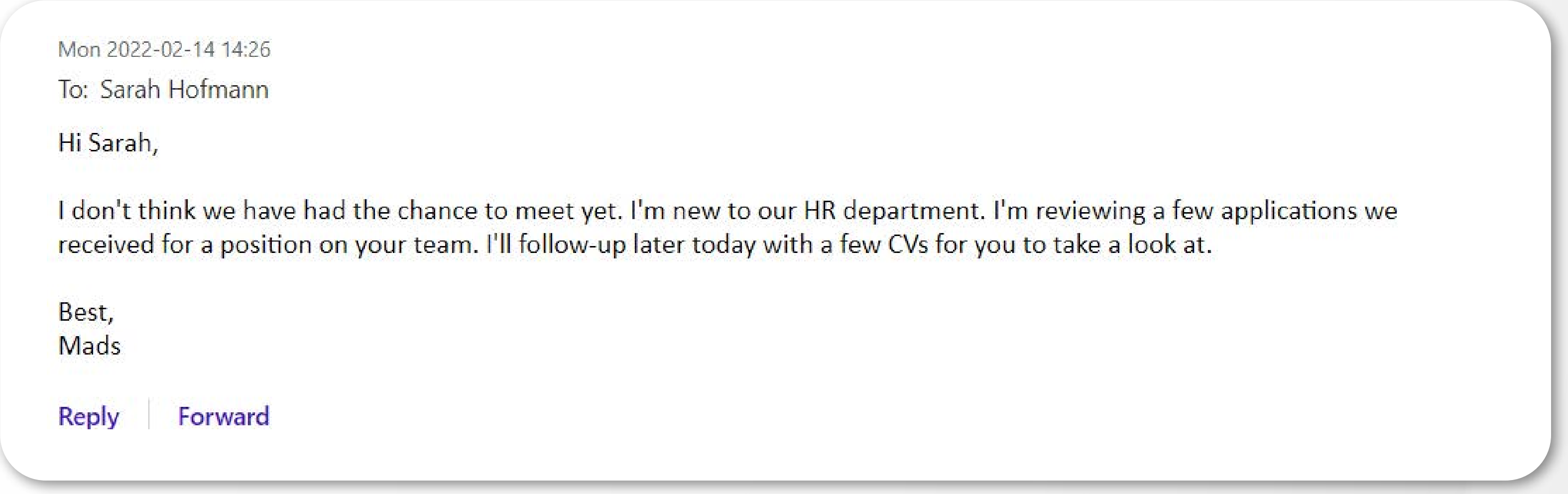
https://tr.im/1Trmg

Smishing

Smishing is very similar to vishing, yet instead of calls or voice messages, it involves text messages or communication apps such as WhatsApp. This strategy similarly uses social engineering in order to impersonate a legitimate institution and instil urgency or even fear in the recipient. A prime example of smishing is a fraudulent message from a bank telling the recipient their account has been compromised. Like the other forms of phishing, the message includes a link that will lead the recipient to a fake website with the aim to steal their credentials.

Barrel Phishing

Also called “double barrel phishing”, this type of attack is designed to build trust with the recipient. The phishing technique involves a lot of research before the criminal strikes. They will then send out a first, non-malicious email impersonating a legitimate and trustworthy organization in order to build a rapport with the victim and make them feel comfortable. Soon after, they will send a second email, this time including a malicious link. Since they have already engaged the victim previously with a non-malicious email, it is more likely that they will manage to compromise their target with the second email after having built trust. Barrel phishing is the first part of a chain of attacks that usually end in financial scams.

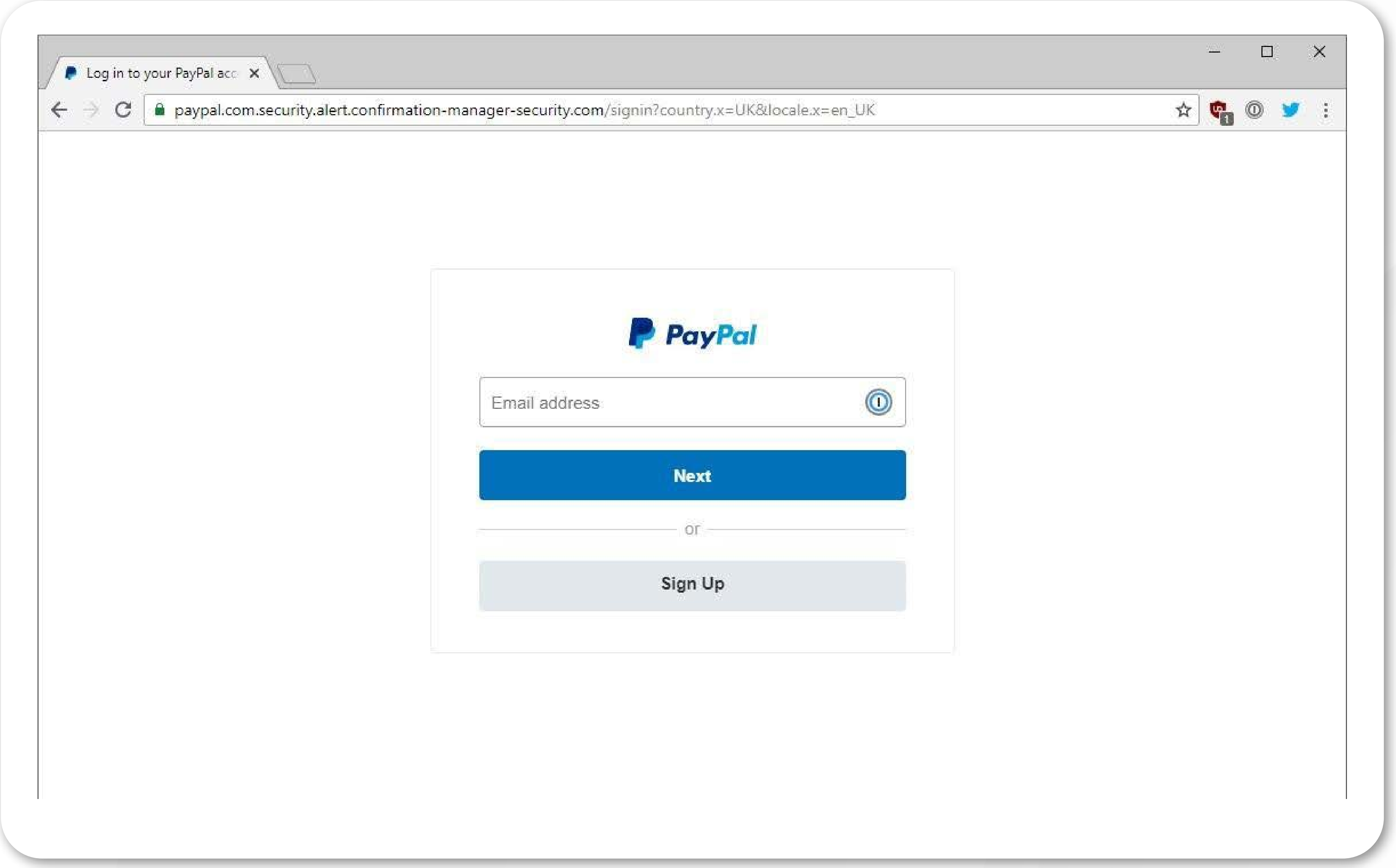


Mon 2022-02-14 14:26
To: Sarah Hofmann

Hi Sarah,

I don't think we have had the chance to meet yet. I'm new to our HR department. I'm reviewing a few applications we received for a position on your team. I'll follow-up later today with a few CVs for you to take a look at.

Best,
Mads



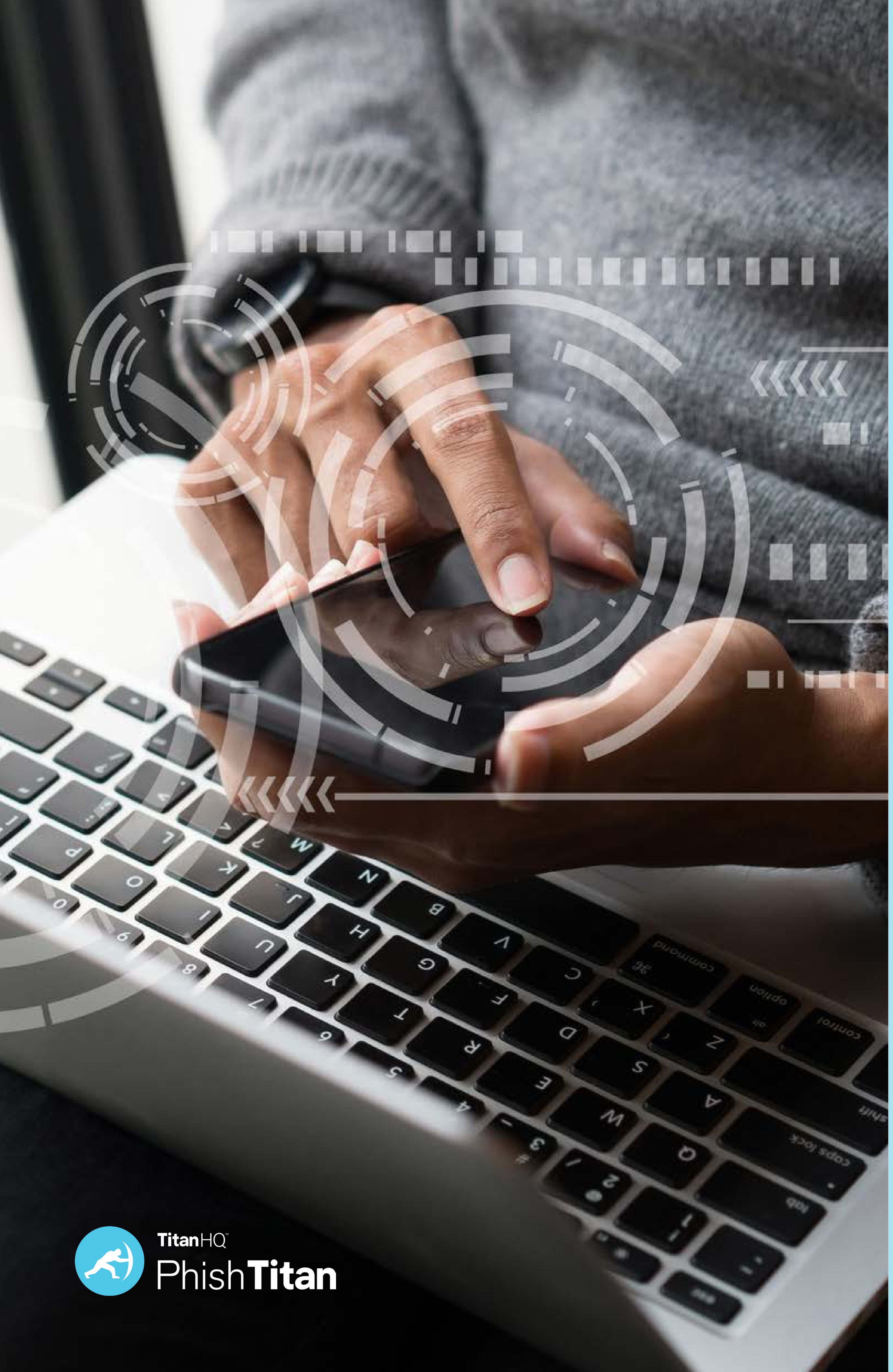
paypal.com.security.alert.confirmation-manager-security.com/signin?country.x=UK&locale.x=en_UK

Fake Websites

Most of the previously mentioned phishing techniques rely on fake websites. These websites are very sophisticated and designed to look almost exactly like the original, and it’s increasingly difficult for most of us to tell the real one from the fake one. The fake websites are created in order to gain login credentials and other sensitive information from the unsuspecting victim and their URLs are linked in most phishing emails. For example: If the victim opens a smishing text message from ‘their’ bank saying the account has been compromised, they will be redirected to a fake website of the bank via the attached link. This is how the criminals can then gain access to the victim’s bank

Educate Your Customers

The most effective way to fight these types of phishing attacks is through awareness. Why not share these examples with your customers to help them be more vigilant?



Layers of Phishing Protections to Keep Your Clients Off the Hook

Phishing is a complex scam that exploits both technical vulnerabilities as well as human error. That's why it's not enough for your customers to simply install anti-virus software and hope for the best. As an MSP, you need to ensure your clients have robust phishing protection in place in order to stop malicious actors from compromising their devices and networks.

Why phishing prevention is crucial

In today's complex cybersecurity landscape, offering robust phishing protections are non-negotiable for MSPs, because:

- It broadens your security portfolio and increases your revenue opportunities
- It protects your clients from the repercussions of an attack
- You're providing greater value and benefits to your clients
- You improve your client satisfaction and long-term relationships

This approach should become standard practice. If your customers aren't willing to adhere to these phishing protection provisions, they put themselves at risk. Not only that, but you, as their MSP, will be the one who bears the brunt of the repercussions should a successful breach occur. Incorporating anti-phishing provisions into your IT support packages does not only protect your clients but yourself as well.

A Multi-Layered Approach to Phishing Protection Includes:

DNS Filtering

One of the most crucial elements of phishing prevention is ensuring your clients have a security solution that includes comprehensive DNS filtering. This provides protection against URL-based email threats, inbox filtering and can rewrite malicious URLs in order to protect users and provide real-time checks on every click.

Phishing Simulations

Theory and practice are very different in most aspects of life, and phishing scams are no exception. Offering phishing simulations to your clients enables them to test their team's abilities and get a realistic idea of how vulnerable their business is to being compromised by malicious actors.

Zero-Day Protection

Offering a phishing protection solution that has zero-day threat protection is crucial. Zero-day threats refer to cyber threats that have not previously been seen and therefore don't match any known signatures. An AI-driven anti-phishing solution will allow you to protect your clients from these modern threats.

Scalable Protection

As evident in vishing and smishing scams, modern phishing is no longer bound to computers only. You need to be able to offer your clients comprehensive phishing protection that's easily scalable across multiple types of devices while still easily configured and updated from a central console.

Robust Authentication

Implementing robust authentication methods is one of the best ways to stop a phishing attack. With multi-factor authentication, your clients can effectively shut malicious actors out. That way, even if they gain access to login credentials, they will not be able to access the account because the authentication comes to another device.

Security Awareness

Human error is one of the biggest factors in successful security breaches. That's why one of the best ways to protect your clients is to offer regular cybersecurity awareness training. Educating teams on modern cyber threats and testing their knowledge will ensure they are better prepared to not fall for phishing scams.

Introducing PhishTitan for Microsoft 365

With over 345 million paying users, Microsoft 365 is one of the most popular application suites for businesses. It is no surprise that it has become a popular target for cyber criminals, and businesses need to ensure a multi-layered security approach that goes beyond Defender.

PhishTitan is our new enterprise-grade anti-phishing service that is designed with MSP specific requirements in mind, including management of multiple clients and ability to react quickly to a threat across multiple email tenants.

PhishTitan enhances your security stance by offering an additional layer of security that complements EOP and Defender. Connecting through M365 APIs, PhishTItan offers effortless onboarding, simple management, additional protective analysis, and the capability for post-delivery remediation across multiple tenants.

PhishTitan offers:

- Native M365 Integration
- Post Delivery Remediation
- Banner Notifications
- Quick Deployment

How PhishTitan Helps Your Reel in Your Email Security

Where threats constantly evolve, a reliable shield is indispensable. PhishTitan enables efficient email protection for MSP's clients by utilizing cutting-edge technology, enhanced detection accuracy, and an array of features driven by the user and customer experience. With PhishTitan, MSPs can confidently navigate cybersecurity challenges with advanced technology solutions and user-centered defense.

Industry Leading Technology

PhishTitan is a cloud based, AI-driven security solution for companies using Microsoft 365, which uses the most sophisticated tools in the IT world to offer comprehensive phishing protection.

It offers advanced features for protection and application management, including:

- URL rewriting
- Time-of-click protection
- Malware protection
- Advanced protection through large language models
- Protection before, during and after the emails journey towards the inbox

Detection Accuracy

Using a combination of detection methods, PhishTitan offers the highest detection accuracy possible. PhishTitan analyzes threats and puts a stop to phishing attacks by providing advanced protection with:

- LLM intelligence and continuous user feedback
- Using curated threat intelligence data that is unmatched in visibility, coverage and accuracy
- URL analysis uses numerous curated feeds to detect malicious destinations linked from phishing mails
- PhishTitan uses Machine learning (ML) detection models that are very effective at adapting to new phishing tactics

MSP Specific Features

We have designed PhishTitan with MSPs in mind. In an increasingly complex threat environment, you need to have the ability to effectively offer email protection to all your customers.

PhishTitan offers:

- Post-delivery remediation — admins will have the ability to remove an email flagged as phishing from single or multiple email boxes
- Management of multiple customers — with PhishTitan, you can quickly react to threats across multiple email tenants and remove phishing emails for multiple clients at once that are very effective at adapting to new phishing tactics

User Experience & Reporting

Using a combination of detection methods, PhishTitan offers the highest detection accuracy possible. PhishTitan analyzes threats and puts a stop to phishing attacks by providing advanced protection with:

- PhishTitan seamlessly integrates into M365 and:
- Offers an additional layer of security that augments Exchange Online Protection (EOP) and Microsoft Defender
- Offers detailed reports and real-time alerts
- Provides automatic bannering of suspect emails and additional feedback using Outlook add-in.

Training & Support

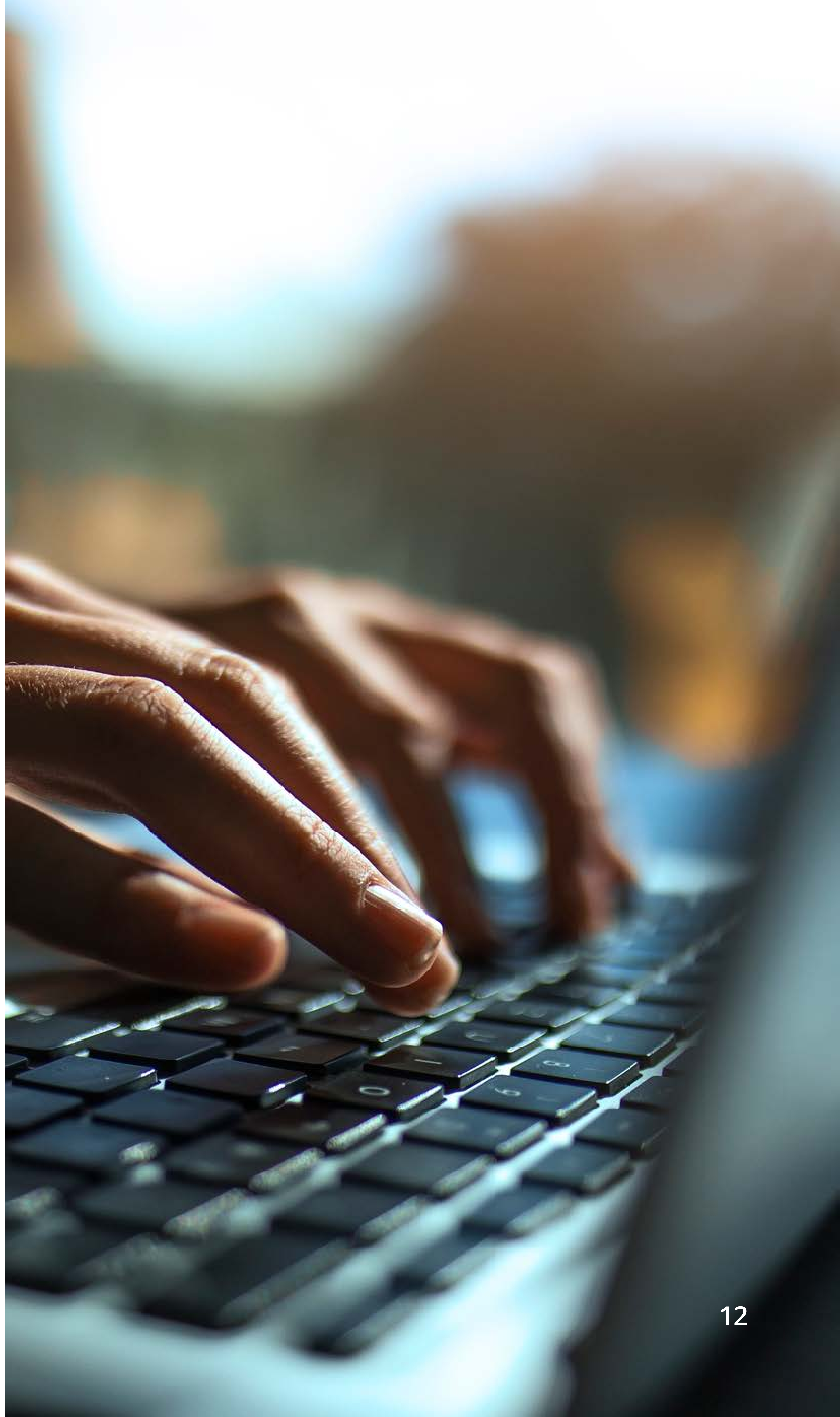
Your clients' teams are one of your most valuable cybersecurity defences. On top of PhishTitan's technical capabilities, we offer extensive customer service, webinars and courses to help you efficiently use our tools and educate your clients about phishing threats.

Next to our robust training resources, our customer support ensures seamless implementation and efficient problem resolution reducing downtime and frustration.

Pricing

Please contact us for pricing information.

Contact Now



TitanHQ
PhishTitan

Bait The Hook to Catch the Phish with TitanHQ

In an increasingly saturated MSP market, we want to help you offer a comprehensive security portfolio in order to stand out from the crowd.

PhishTitan does just that—it's designed to deliver unbeatable anti-phishing accuracy, minimal false-positive results and ease of use. Are you ready to learn more about PhishTitan's superior protection capabilities?

Get in touch with us today to discover its powerful potential and book your demo today.

Get in touch