DASHLANE

Phishing 101 Guide

A Six-Step Action Plan to Prevent Employees From Taking the Bait

Scare tactics are common in cybersecurity. After all, emotions are a powerful motivator, and a little tale about a big phish can resonate. But at the end of the day, negative emotions won’t help you build a positive culture of cybersecurity awareness.

Educating employees on phishing

When it comes to phishing initiatives, creating awareness with fear tactics often makes employees annoyed at your IT team—or worse, resentful. They may even feel so anxious about phishing that they won't click on any link or attachment—even important ones.

So if the goal is to scare employees so much that they stop opening the PowerPoints that the People team emails every quarter, then mission accomplished. But if the goal is to promote positive cybersecurity awareness, there are more inspiring and effective ways than shaming and scare tactics.

What can you do instead? Nurturing a blame-free, empowering security culture takes a consistent effort. We've created a six-step action plan that guides you through the elements of a successful education and training program to prevent phishing and inspire your employees.

"I always shock people when I tell them the best tool you can have is a human-first mindset: treating your employees with respect and providing them with the right knowledge and software. [...] It is important to view employees as internal customers."

—Naya Moss, Founder, Frauvis

Read the full interview with information security pro Naya Moss here

Section 1

Phishing 101

A fisher may know how to hook the audience with a good fib, but a phisher knows how to get people to take the bait. Cybercriminals are strong storytellers, psychologists, and marketers rolled into one. But it's not those diverse talents that make phishing their favorite hobby—it's the promise of a big catch.

If simulated phishing tests are any indication, **a third of people who receive a phishing email will click on the link or open the attachment.**[1] Phishing works because it taps into some of the most-basic human traits—curiosity, carelessness, fear of missing out—and scammers know how to use those traits to their advantage.

The first mass emailed phishing campaign, launched in May 2000, caused up to an estimated $10 billion in damages. The now infamous ILOVEYOU virus, which infected millions of computers, came as an executable text attachment in a simple, albeit irresistible, message: "kindly check the attached LOVELETTER coming from me." More than two decades later, scammers use the same core techniques (and often bad grammar) to reel in unsuspecting victims. But their tools have improved significantly, making phishing one of the most commonly used attack vectors.

[1] Keepnet Labs, "Phishing Trends Report," 2020

Top consequences from a successful phishing attack

Percentages indicate the ratio of surveyed organizations that experienced each situation.

60%
data loss

52%
credential or account compromise

42%
ransomware infection

29%
other malware infection

18%
financial loss or wire transfer fraud

Source: "2021 State of the Phish," Proofpoint, 2021

In 2021, 83% of U.S. organizations said they experienced a successful phishing attack.[2] Companies providing business-related applications were the most frequently impersonated (also known as brandjacking). These companies—including Zoom, DocuSign, and Microsoft—accounted for 45% of brandjacking-related phishing.[3]

These trends sound unsettling—but by educating and training your employees, you will empower them with the knowledge to avoid taking the bait.

> "We saw a 35% increase in our security incidents, mainly phishing attacks, in 2020."
>
> —Heather Hankins, Security Specialist, NETA

[2] Proofpoint, "2022 State of the Phish," 2021

[3] GreatHorn, "2021 Email Benchmarking Report," February 2021

A deeper dive into phishing attacks

The word phishing is commonly used as an umbrella term for several varieties of attacks, though the overarching category is considered social engineering. Social engineers prey on human nature with the goal of manipulating a person to take specific action. Although digital technology has made social engineering ubiquitous through phishing, this deception technique dates back thousands of years.

One of the most successful social engineering schemes in the past was done by George Parker, who, like today's scammers, pounced on the opportunity to capitalize on a current event—the 1883 construction of the Brooklyn Bridge in New York.

One tale claims that as soon as the bridge was finished, Parker started "selling" the structure to unsuspecting customers at least twice a week for $50–$55,000, even offering to show his certificate of ownership; that's the equivalent of about $1.3 million today.

He also "sold" other landmarks, like the Statue of Liberty and Madison Square Garden—but he left his true mark by giving us the phrase "I have a bridge to sell you…" And countless generations of social engineers have been selling bridges ever since.

The social engineer’s tackle box

The bait

A fake communication, often impersonating an individual or brand

The lure

A malicious link or attachment

The reel

Social media trolling and other research

The hook

An email (most common), text message, phone call, or social media message

The rod

Phishing kit and automated tools

The catch

Stolen login credentials or a compromised system

Types of phishing

Phishing

In addition to being used an umbrella term for all phishing attacks, phishing refers to the most common type: fraudulent emails sent to a large number of people. The idea is to cast a wide net with simple bait—generic messages. Attackers can easily find off-the-shelf phishing kits that come complete with all the tools they need.

Why it works: Attackers spoof email addresses, impersonate brands, and use typosquatting (look-alike URLs) and other methods to create authentic-looking emails that hook recipients with urgent, confusing, or mysterious messaging.

Smishing

Smishing is a phishing attack sent via text messaging or SMS. Attackers use a fake phone number and may impersonate a legitimate company. The link in the message often takes the recipient to an authentic-looking site that may request sensitive information or prompt a malicious download.

Why it works: Many people tend to trust a text message more than an email. And since smishing is less common, it's easier to catch someone off-guard.

Spear phishing

To improve their chances of a catch, cybercriminals use better bait —such as personalized, bespoke emails—aimed at specific individuals or companies. The attackers may take an educated guess or search social media for relevant information that will create a more believable message. This attack is more complicated to execute but yields better results.

Why it works: Because the experience is tailored to the targeted individuals or businesses, the recipients are more likely to click on the link or attachment.

Vishing

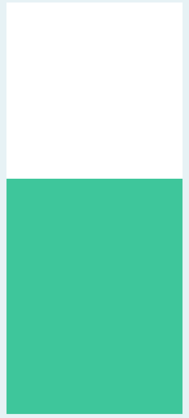
A type of phishing or spear phishing carried out via a voice call, vishing may involve either a live caller or a robocall. The call typically has a sense of urgency and often impersonates a government authority or financial institution. The scammers can spoof a phone number and either dial random numbers en masse with automated methods or make personalized calls to a specific person after researching information about the potential victim.

Why it works: Caught off-guard, the target reacts in the moment and doesn't have time to assess the situation—or they become too confused or flustered to spot a red flag.

Whale phishing

Also known as whaling, whale phishing is spear phishing that goes for the biggest and best catch: a high-value member of a company, such as a C-suite executive. These "whales" are harder to catch; but since they have more access to sensitive or restricted resources, landing one can pay major dividends.

Why it works: Whale phishing is a well-planned attack that starts with gathering details about the target's personal and work lives, habits, and patterns. It relies on gaining the target's trust, potentially over a longer period of time.



39%

of people reuse passwords across workplace accounts

Source: Yubico and Ponemon Institute, "The 2020 State of Password and Authentication Security Behaviors Report," February 2020

Spot the difference

An especially problematic type of phishing is **clone phishing**. Difficult to detect, this attack uses a cloned copy of an existing, legitimate email with an “updated” message to trick the recipient into believing it’s a revision due to an error in the original email. The replicated message comes either from a spoofed email address or one that’s nearly identical, and a malicious link or attachment replaces the original one.

Section 2

Gone phishing

Five new types of bait to watch out for

As people get better at spotting phishing attacks, scammers find new ways to entice clicks. Here are just a few of the latest phishing bait varieties that emerged in the last year or so.

The reCAPTCHA phish

In December 2020, researchers spotted a Microsoft-themed phishing campaign that used fake Google reCAPTCHA to harvest the credentials of senior company employees. The targets received an email message that appeared to originate from their unified communications system. The .html attachment sent the recipient to a malicious website that "verified" the reCAPTCHA, then loaded a fake Microsoft login page.

The FedEx phish

Many people know better than to click on fraudulent shipping email notifications, so scammers upped their game in 2020. They hosted their malicious websites on the reputable Quip platform, an add-on Salesforce tool that many businesses use for files. The email, impersonating FedEx, claimed the target had a scanned document to review. The link sent the recipient to the Quip platform, and if the person clicked the prompt to review the file, the site redirected to a fake Microsoft login portal.

The coronavirus-themed phish

Because the coronavirus is such an emotionally charged topic, it proved to be a highly effective lure. Starting in 2020, phishing emails with false vaccine and stimulus check information began making the rounds en masse. Proofpoint reportedly blocked millions of coronavirus-themed phishing emails in 2020 alone and considers this theme the second most-used of that year.

The "customized DIY" phish

A novel phishing toolkit called LogoKit emerged in 2021, and it allows attackers to create phishing pages in real time—customizing the logos and other content based on the recipient's email domain. The kit also autofills the email so it appears the person had already visited that website. Once the individual enters their password, the page redirects to the legitimate corporate site. Researchers observed the tool in the wild, and it was installed on 300 domains in just one week and on about 700 sites in one month.

The "pumpkin spice latte" phish

Nearly 100% of recipients clicked on a phishing link that came in an email promoting the Starbucks pumpkin spice season. Alright, we confess: This was not an actual campaign (that we know of). But in simulated phishing tests sent in 2020 to at least 2,300 employees, this was the third most-clicked theme (right after "a free month of Netflix" and "a vacation contract rental"), according to security company Proofpoint.[4] Other successful phishing topics that got employees to click included "dress code violations" and "Spotify password update prompt."

[4] Proofpoint, "2021 State of the Phish," 2021

How big companies found themselves in deep water

Colonial Pipeline

In spring of 2021, a major U.S. oil pipeline was taken offline for over a week due to a cyberattack. The attack caused shortages across the country—and was caused by one stolen employee password. While we may never know exactly how the hacker obtained the password, the U.S. Cybersecurity & Infrastructure Security Agency (CISA) suspects the cyberattackers gained entry through ransomware sent in phishing emails. Part of the reason they suspect this is because email-based attacks have been behind other high-profile infrastructure attacks in the recent past.

FACC

The Chinese-based airplane-parts manufacturer suffered one of the costliest phishing attacks in history after it was fooled into transferring $61 million to foreign accounts. In an example of business email compromise, bad actors impersonated the CEO and sent a phishing email to an entry-level employee in accounting, authorizing the transfer for a bogus project. FACC later sued its former chief executive and chief financial officers for $11 million, saying they didn't implement enough controls to prevent the fraud.

U.S. infrastructure sectors

In 2016, a multi-stage phishing campaign affected multiple organizations in the U.S. power grid and critical infrastructure sectors. While the main targets were U.S. government entities, the Russian government actors behind the attack first compromised smaller companies that had relationships with those agencies, stealing credentials and gaining access into networks. Two years later, the Department of Homeland Security and the Federal Bureau of Investigation issued an alert detailing the attackers' tactics, techniques, and procedures (TTPs).

Levitas Capital

In a more recent example, the Australian hedge fund Levitas Capital went out of business in 2020 after a phishing attack resulted in the payment of $8.7 million worth of fraudulent invoices. The attack began with one of the co-founders receiving a fake Zoom invite link. The malicious link led to a malware download, enabling the scammers to take control of the email system and generate fake invoices from legitimate companies. The attackers then spoofed the co-founder's email address to approve the invoices.

GoDaddy

The popular website host's employees are a frequent target of social engineering, and 2020 was no different. In March, a spear phishing email sent to a customer service employee resulted in the bad actor gaining access to customer records. The attackers modified the domain settings for many customers, including escrow.com, which brokers online transactions and integrates with platforms like Shopify and eBay. As part of the hack, the escrow.com home page was redirected to a website that displayed a profane message.

Section 3

A six-step action plan to keep employees off the hook

Phishing may be no laughing matter—but humor is a more powerful (and positive!) motivator than fear. As you start on your action plan, we recommend adding some bites of humor to your awareness program.

And at the very least, consider leaving out penalties. More than half of organizations punish users who chronically fall for simulated phishing attacks; of those that do, only 47% said this consequence model has widespread employee acceptance.[5] That means more than half of employees are uncertain, unhappy, or angry about the idea.

As two U.S. and U.K. academic researchers recently discovered, scare tactics used for cybersecurity awareness "don't get people invested in security over the long term."[6] They also found that 21% of the research participants agreed fear-based appeals were not necessary.

According to the researchers, there are different tactics that work better: trust and creativity. And those are the perfect components of a strong security culture—which takes us to the first step of our action plan.

[5] Proofpoint, "2021 State of the Phish," 2021

[6] Wall Street Journal, "Why Companies Should Stop Scaring Employees About Cybersecurity," December 7, 2020

STEP 1

Create a culture of security

A culture of security shouldn't mean sacrificing productivity. In a security-first culture, employees:

- Understand their roles in protecting your company's data and IT resources
- Are active participants in ongoing security conversations
- Have the tools they need to maintain good security habits without impeding their work

A blame-free culture doesn't mean lack of accountability. Instead of using a punitive model, however, find other ways that motivate employees to follow policies and good security habits.

A recent Dashlane and Harris Poll survey found that 79% of employees take at least some personal responsibility for their company's overall security.[7] Employees want to be part of the solution, and you need to show them how they can do that.

> "One of our biggest concerns is phishing emails."
>
> —Ben Leibert, Technical Manager, VillageReach

Learn how VillageReach used Dashlane to build a culture of security that protects them from phishing attacks and other cybersecurity concerns.

[7] Dashlane, "New Research Uncovers the State of Security in the Workplace," 2020.

Do this, not that

Quick tips for successfully building a security culture

Fail: Instill fear in employees by fining them with salary deductions or firing them for repeatedly falling for simulated phishing. Or embarrass them by posting their photos in a shared space for public shaming. (Yes—these are real examples.)

Success: Implement a buddy system that appoints a peer to be a team's cybersecurity expert. This person receives additional training and can answer questions about threats and help employees when they experience issues like a potential phishing attack. A "buddy" is less intimidating than a team manager or IT admin.

Fail: Require employees to use strong passwords that they can't reuse or write down—without giving them a way to securely manage their credentials. This is a recipe for employee anxiety, policy circumvention, or both.

Success: Provide appropriate resources, such as a password manager, so employees can use and manage strong passwords. Implement a messaging system that immediately alerts everyone (not via email) when an employee spots a phishing attempt. And instead of banning the tools that employees love, find ways to use those tools securely.

Adapted from Karen Renaud, University of Abertay, Dundee, U.K. researcher, as published in the Wall Street Journal, "Why Companies Should Stop Scaring Employees About Cybersecurity," December 7, 2020

STEP 2

Implement a cybersecurity education, training, and awareness program

A successful cybersecurity education, training, and awareness program needs to answer these five questions:

1. Why does security matter to your company?
2. Why should employees care about security?
3. How do cybercriminals target and attack businesses like yours?
4. How can employees help prevent these attacks?
5. What actions can employees take in the course of their daily work to enhance security?

And remember: No one's ever hooked on PowerPoint presentations, no matter how much you entice people with free pizza. And employees likely won't read long documents about security. To engage them, use a combination of training modules, with a focus on interactive sessions—and consider adding an element of entertainment.

Keep security top of mind by:

REMINDER 2m ago

Integrating education and awareness as part of new hire onboarding

REMINDER 3m ago

Providing refresher trainings at a regular cadence

REMINDER 5m ago

Sending quick tips and reminders through internal communication channels

REMINDER 8m ago

Sharing relevant news about data breaches and hacks that involve social engineering, with tips for how to avoid taking the bait

Adapted from Karen Renaud, University of Abertay, Dundee, U.K. researcher, as published in the Wall Street Journal, "Why Companies Should Stop Scaring Employees About Cybersecurity," December 7, 2020

STEP 3

Conduct simulated phishing campaigns

To help employees recognize phishing and risky actions through first-hand experiences, use a “show, don’t tell” approach with simulated phishing tests. By conducting regular mock phishing campaigns, you can turn employees from a weak link in company security to a point of strength.

In addition to serving as practice for employees, the phishing tests measure how many people open the emails, click on the links and attachments, and complete the final action (such as entering their login credentials). You can use these metrics to track the effectiveness of your program over time and identify areas that need additional education and awareness.

A few tips for conducting simulated phishing:

- Don’t limit the phishing test to just an email. Include vishing, smishing, and other methods that can reel people in.
- Be creative with your themes. As we saw earlier, a Starbucks or free Netflix phish is highly tempting.
- Resist a “gotcha!” approach. Use these tests as an opportunity to educate and reward secure behavior. One idea is to have a department contest with a reward—and get extra points for something besides the usual free lunch.

An insider’s tip to prevent phishing

Dashlane recently hosted a Q&A with Rachel Tobac of SocialProof Security, an ethical hacker who infiltrates companies with social engineering techniques to help them strengthen their people defenses.

“One of my biggest jobs is helping people become politely paranoid, so figuring out, according to their threat model, how much polite paranoia they need to incorporate into their work and their personal life. For a person who is not in the public eye, posting a picture of yourself drinking a mojito on the beach is completely fine but I would say, how about we don’t tag the hotel, so that I don’t know who to call to get information about you. If you don’t tag the hotel, then I don’t know who to place the call to, pretend to be you, and gain access to where you’re staying and what room number you’re in.”

—Rachel Tobac, CEO, SocialProof Security

Want access to the entire event? Grab a drink, a snack, and maybe a hack with Rachel Tobac.

Watch now or save for later →

STEP 4

Tailor your program to different job functions

Phishers may not always have perfect spelling, but they shine at psychology and human behavior. And they’re meticulous researchers. That’s why they won’t send a spear phishing email with a fake resume to Jordan in accounting or an invoice to Sam in marketing. And neither should you when you’re conducting simulated phishing.

In addition to educating employees on universal security topics that apply to everyone, provide custom training to different teams and departments based on their roles and job functions. And don’t forget your “whales”—those high-value targets who need to be extra vigilant.

Who takes the bait?

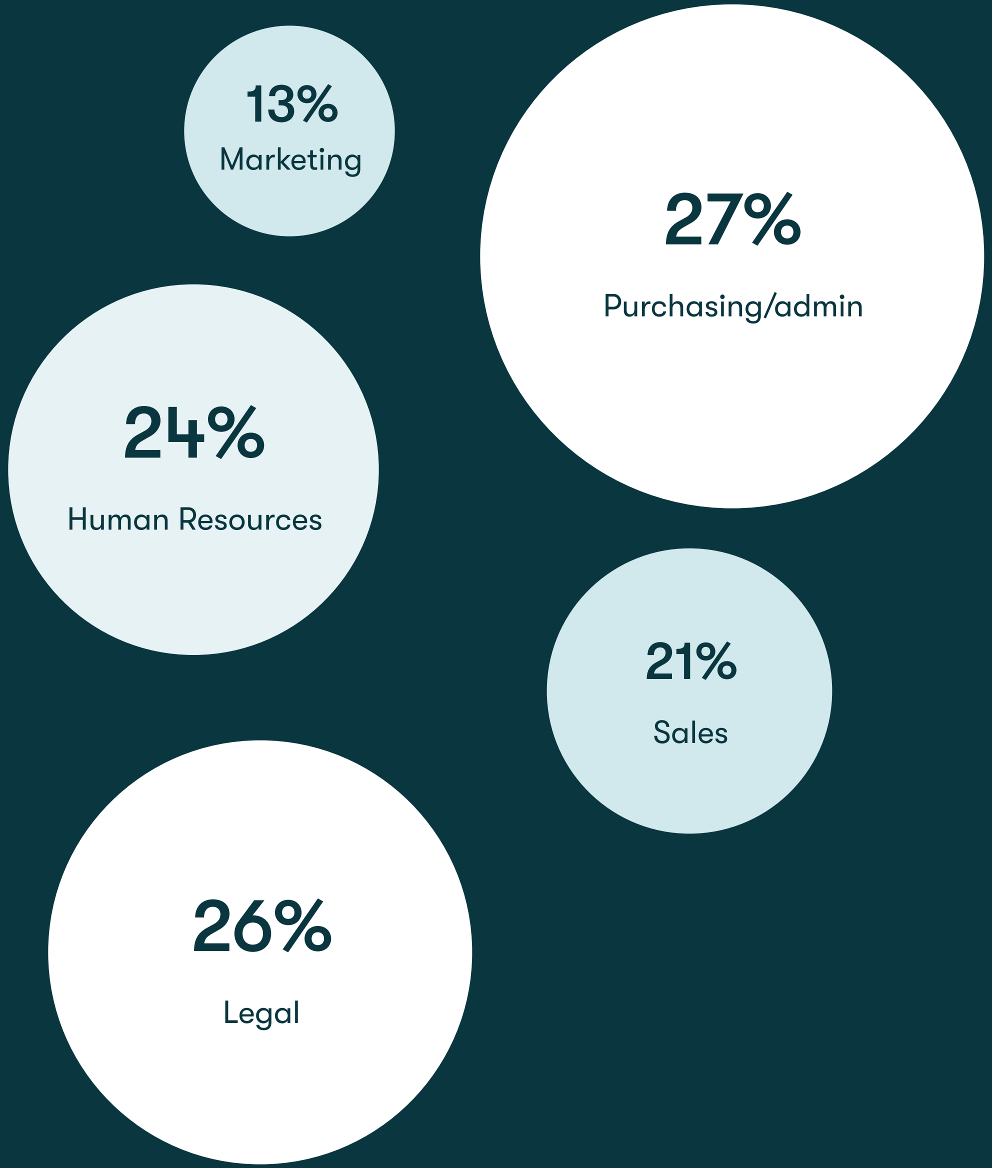
See how different departments interacted with simulated phishing tests.

	Human resources	Purchasing/ admin	Sales	Marketing	IT	Finance	Legal
Opened	72%	77%	73%	48%	58%	42%	78%
Clicked	55%	59%	53%	32%	20%	26%	59%
Submitted info	24%	27%	21%	13%	8%	7%	26%

Source: Keepnet Labs, “2020 Phishing Trends Report,” 2020

Who gets caught?

A percent of all these departments submitted info during simulated phishing tests.



STEP 5

Boost phishing defenses with additional tools and processes

Education and awareness are empowering. But at the end of the day, you still need to provide tools and implement processes that support and promote secure practices.

There's no perfect recipe for this step, but there are a few simple tips recommended by the NIST cybersecurity framework you can use to create a plan tailored to your environment and objectives:

- Adopt technology such as endpoint security, password managers, and email security. These technologies, among others, will minimize the impact and damage from phishing attacks.
- Many successful phishing attacks end with malware installed on a victim's device. Maintain a regular patching schedule for all apps, devices, and other systems to eliminate vulnerabilities that malware can exploit.
- Train employees how to identify and report suspected security incidents and threats, including suspected phishing attacks. Consider creating a special email or channel for them to reach out to.

Don’t take the bait

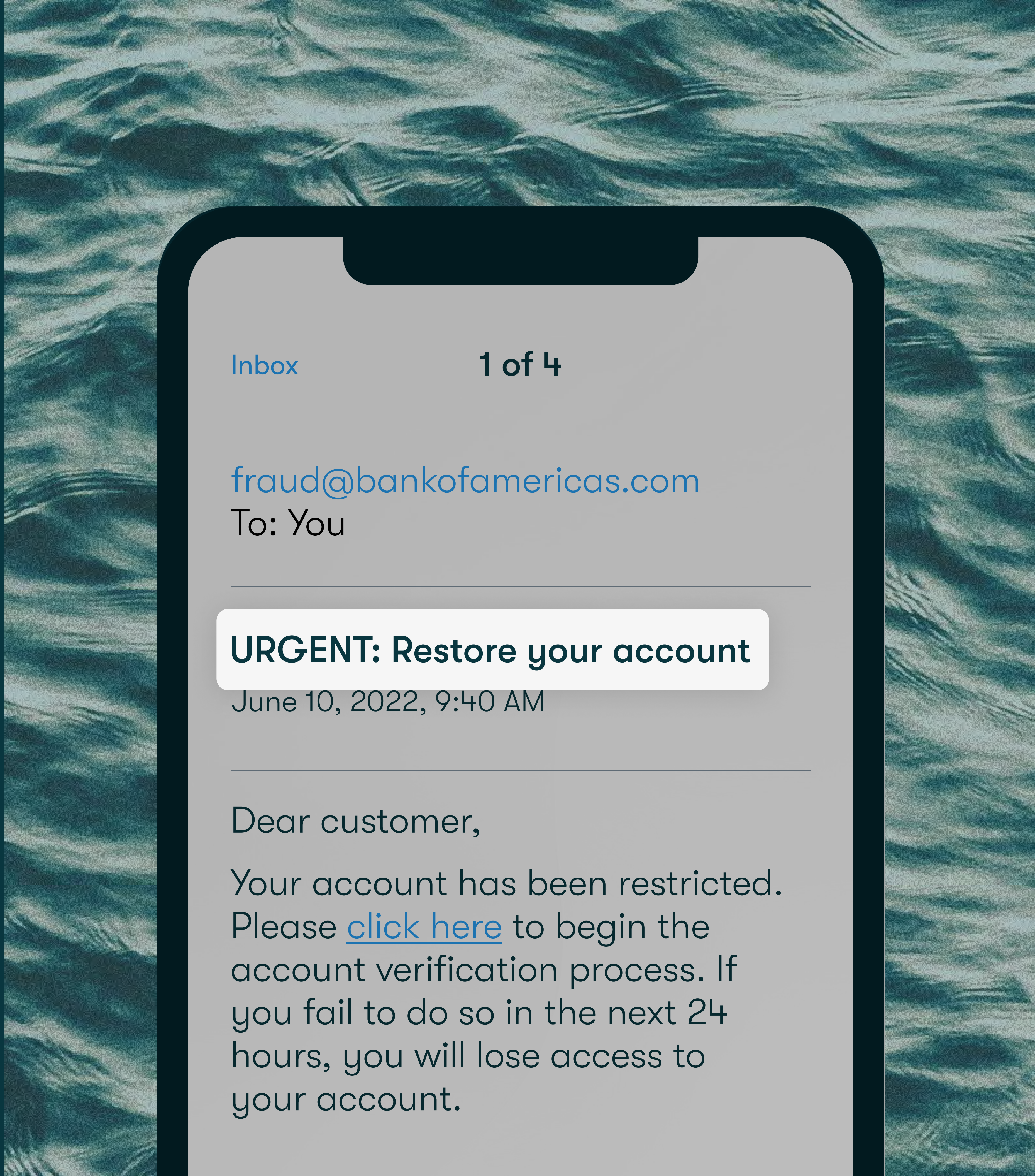
Helpful tips for spotting a phishing attempt based on an email's subject line, sender name, message body, and requested action.

The subject line

What to check before you click:

- → A sense of urgency
- → Scare tactics
- → Enticing offer

Remember that scammers prey on curiosity, current events, fear of missing out, and anxiety.



Inbox 1 of 4

fraud@bankofamericas.com
To: You

URGENT: Restore your account
June 10, 2022, 9:40 AM

Dear customer,

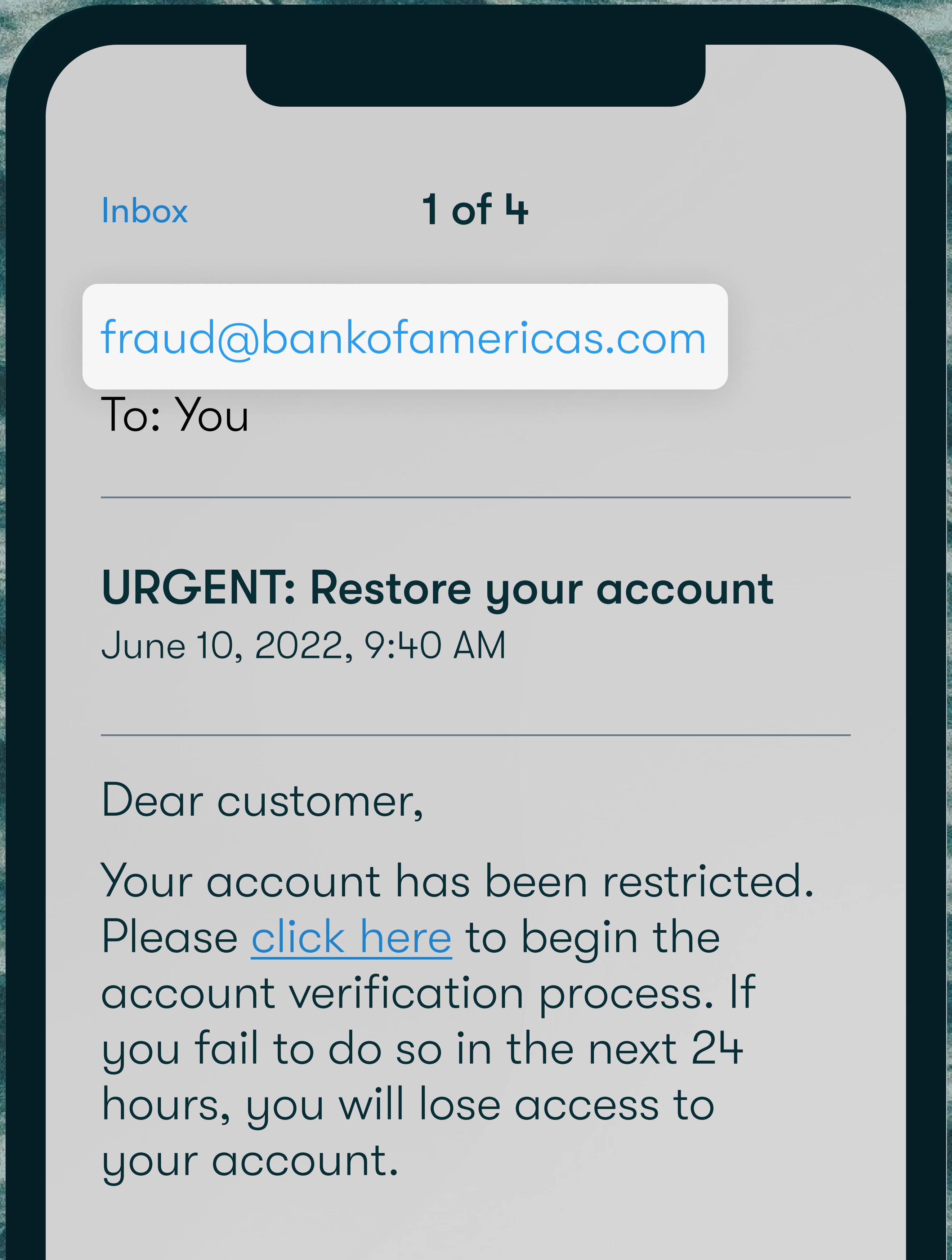
Your account has been restricted. Please click here to begin the account verification process. If you fail to do so in the next 24 hours, you will lose access to your account.

The sender

What to check before you click:

- → Email address that doesn't match the person's name
- → Email domain that doesn't match the sender's company
- → Lookalike but suspicious email domain

Hover over the sender field to reveal the email address. And remember, scammers can also spoof an email, so be wary if you see the other red flags—even if the address looks legit or appears to come from someone you know.



fraud@bankofamericas.com

To: You

URGENT: Restore your account

June 10, 2022, 9:40 AM

Dear customer,

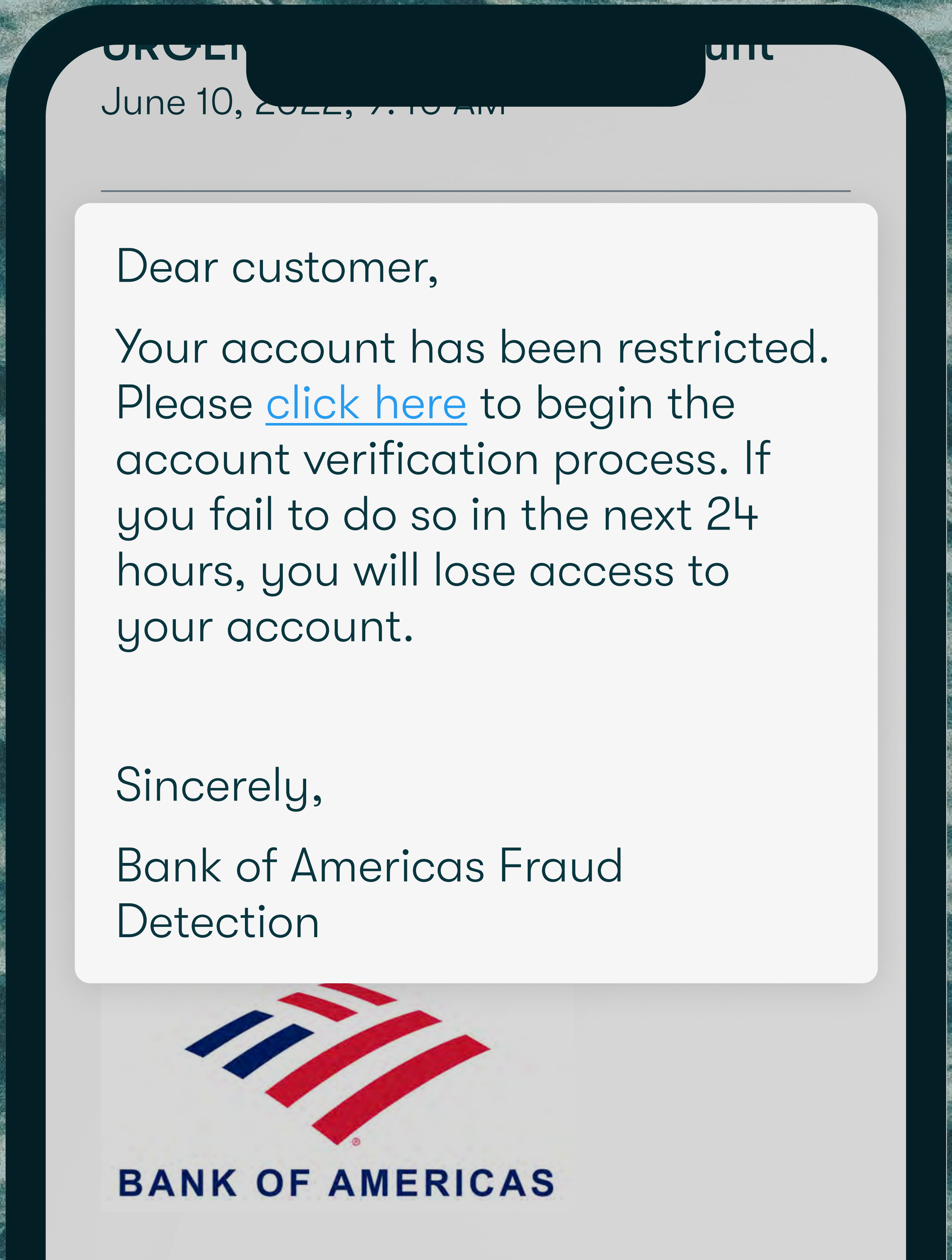
Your account has been restricted. Please click here to begin the account verification process. If you fail to do so in the next 24 hours, you will lose access to your account.

The message body

What to check before you click:

- Lack of personalization (doesn't have your name)
- Poor spelling and grammar, or unusual/awkward use of language

Your bank or another company you do business with is not likely to address important personal correspondence to "dear customer." But don't be fooled by personalization either, because scammers can also learn your personal details.



June 10, 2022, 9:10 AM

Dear customer,

Your account has been restricted. Please click here to begin the account verification process. If you fail to do so in the next 24 hours, you will lose access to your account.

Sincerely,

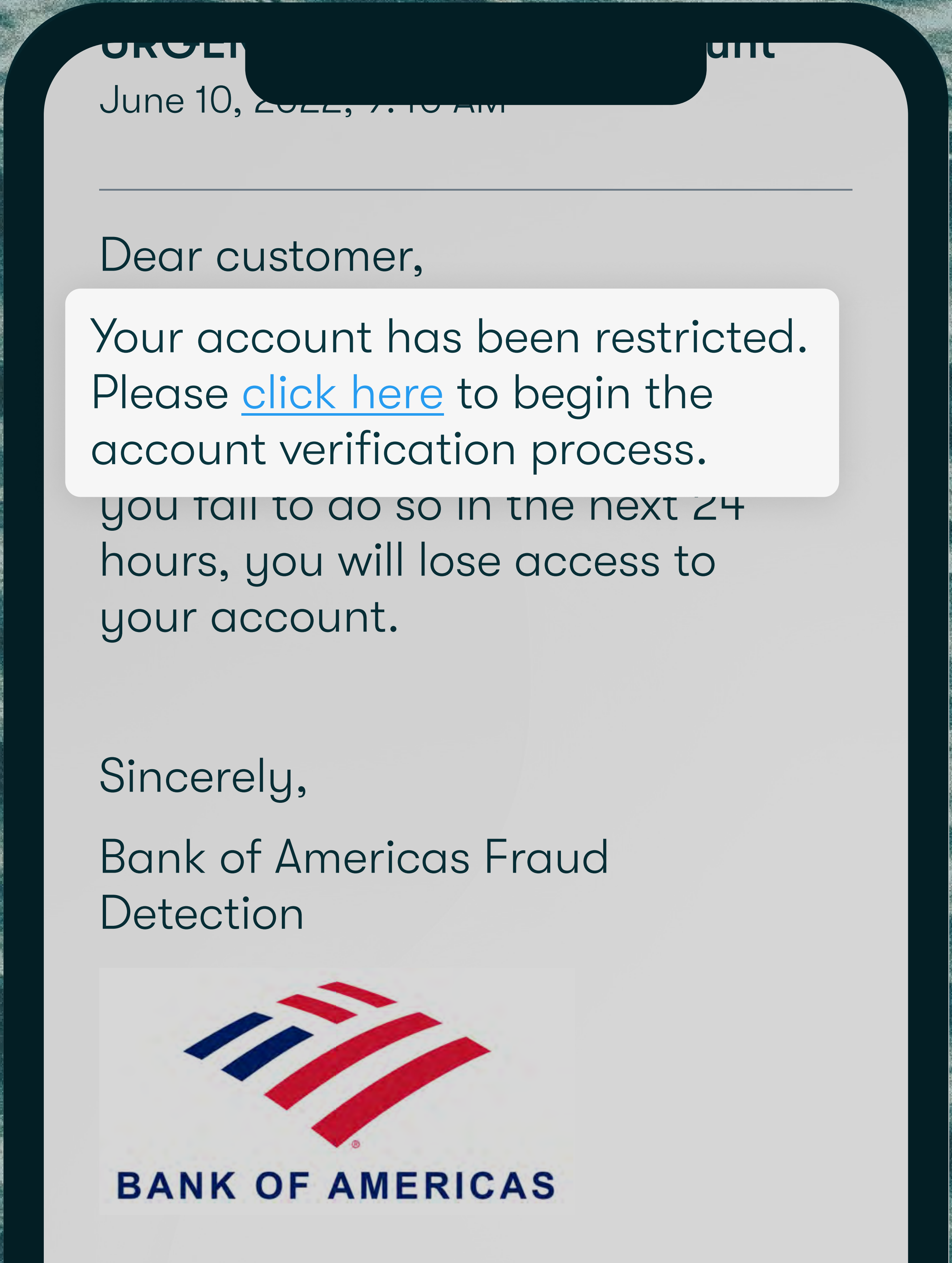
Bank of Americas Fraud Detection

The requested action

What to check before you click:

- → Unusual or strange claim, such as a notice that your account was locked, an invoice you don't expect, or a message from a company where you don't have an account
- → Request for sensitive information, such as logging in to verify your account
- → A link that looks suspicious, such as a shortened, lookalike, or mismatched URL

Hover over the URL to reveal the true destination and if anything feels off, don't click on it or open the attachment. Contact the company directly by using the number listed on the company's website. If the suspicious message appears to come from someone you know, call that person directly. For a short URL, use an online shortened URL decoder to reveal the full address.



June 10,

Dear customer,

Your account has been restricted. Please click here to begin the account verification process.

you fail to do so in the next 24 hours, you will lose access to your account.

Sincerely,

Bank of Americas Fraud Detection

STEP 6

Measure effectiveness and iterate

A cybersecurity awareness program without metrics is like a catch and release—but without a picture. You can't really prove anything. To see how well your efforts are working, you need a baseline at the beginning of implementation and periodic measurements thereafter.

Quantifying cybersecurity posture is not necessarily easy, so you may need to think out of the box. Don't use the simulated phishing click rates as the only metric, because that doesn't provide a holistic picture. Besides, some employees are just too busy to read emails so you may have outliers who will skew your results.

Your tools may also provide ways to creatively measure your program's effectiveness. For example, some password managers include a password health feature that tracks your companywide password security scores over time.

Security education and awareness building is not a "one and done" endeavor. To achieve your desired outcomes, measure impact—whether using concrete numbers or informal feedback—and regularly adjust your strategy based on results.

CONCLUSION

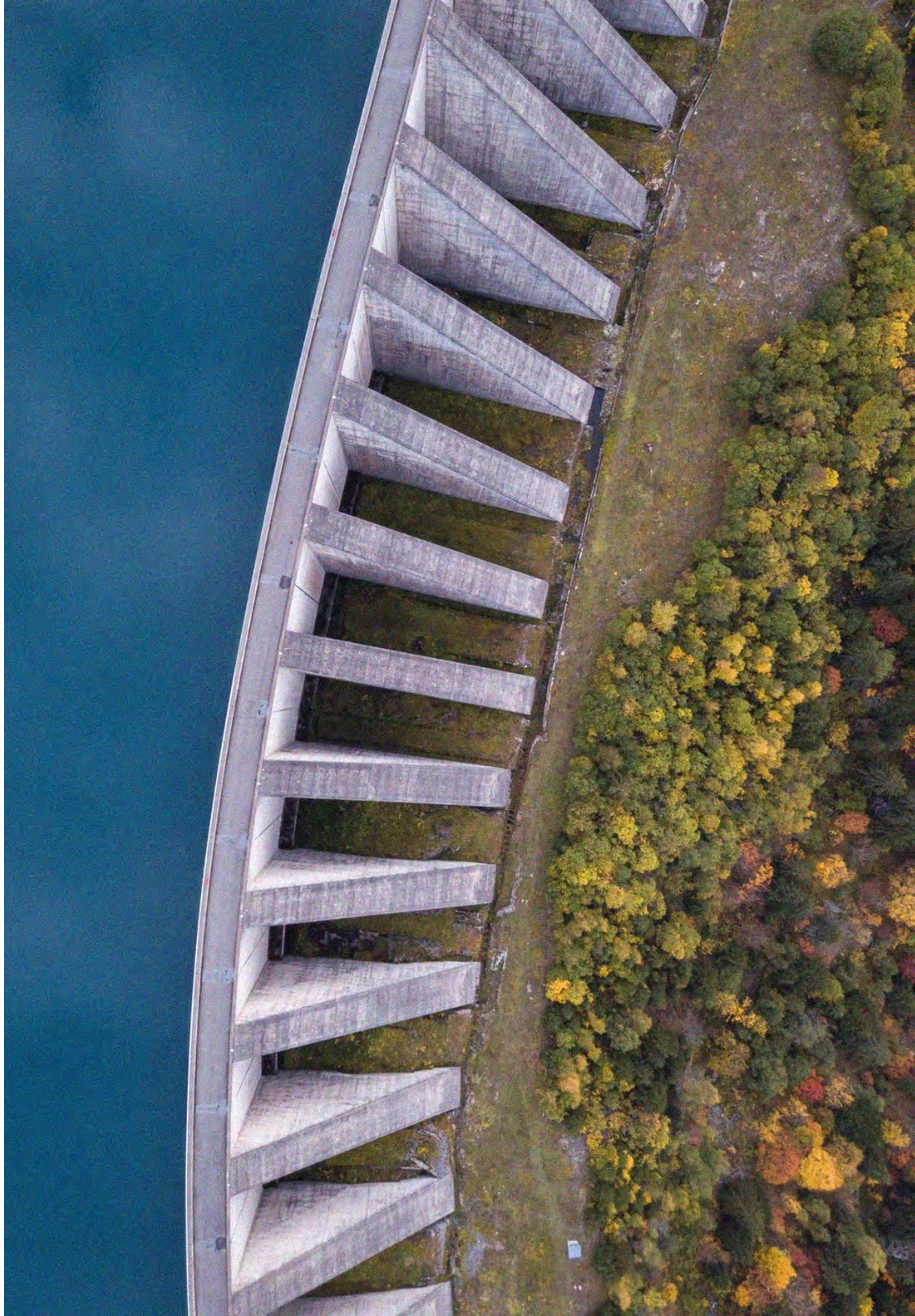
Your best line of defense

Many businesses are improving their security technologies and processes to make it harder for phishers to hook their employees. But phishers will continue to find novel, unexpected ways to lure people with social engineering.

Your best defense is planning for the unexpected and empowering employees with current knowledge, appropriate tools, and ongoing awareness.

Want to learn how you can strengthen your security and protect your business when phishing compromises employee passwords? Download our e-book, “A Practical Guide to Cybersecurity with a Password Manager.”

Ready to test out a password manager? Get a free trial, on us →



DASHLANE