24
Feb

hing

19 Examples of Common Phishing Emails

A shocking proportion of email traffic—about 49% according to 2022 data—is spam. Much of that spam is purposely crafted for fraudulent purposes, to compromise communication, and gain access to data, networks, or funds.

Many spam filtering programs identify spam messages before they reach human readers. Many more seem obviously fishy and are easy to delete when they reach your inbox. But what about those outlier messages that are hard for both software and people to detect?

Based on the latest 2022 Gone Phishing Tournament results, in an organization of 10,000 or more employees, 690 are likely to click on a phishing email link.

For small businesses, this translates to 3 or 4 individuals falling for the "phish" and giving out confidential information. For businesses, those actions by a small minority of employees can cause maximum damage.

Being able to consistently detect and avoid phishing emails that arrive in your inbox or appear on your smartphone is a key component of strong cyber security. To do that, it's important to be aware of different types of phishing emails and stay attentive to the warning signs in every possible scenario.

What is a Phishing Email?

A phishing email is a cyber attack that relies on deception to steal confidential information from users and organizations.

Phishing victims are tricked into disclosing information that should be kept private. When a phishing email arrives, recipients have no reason to doubt the request. They believe that the party requesting the information – often posing as a familiar platform, a trusted vendor, colleague, or boss – is who they say they are. With the best intentions, phishing email victims respond without a second thought.
In phishing emails, cyber criminals often ask for the following information:

- Date of birth
- Social security number
- Phone number
- Home address
- Credit card details
- Login details
- Password (or other information needed to reset your password)

Cyber criminals then use this information to impersonate you and apply for credit cards or loans, open bank accounts, and commit other fraudulent acts.

Some cyber criminals use the information collected in an initial phishing email to launch more targeted cyber attacks, such as spear phishing or business email compromises (BEC), that rely on knowing more about the victim.

How Does Phishing Happen?

Phishing happens when a victim acts on a fraudulent email that demands urgent action.

Examples of requested actions in a phishing email include:

- Clicking an attachment
- Enabling macros in a Word document
- Updating a password
- Responding to a social media friend or contact request
- Connecting to a new Wi-Fi hot spot

Every year, cyber criminals become savvier with their phishing tactics, improve their techniques, and try new methods to deceive and steal from unsuspecting people. Now you can expect phishing through voicemails and texts, in addition to emails.

How many employees fall for common phishing threats?

Search

Search...

Categories

- Compliance and Governance (9)
- Cyber Security Awareness (298)
- Data Privacy Awareness (57)
- Events (11)
- GDPR (9)
- News (25)
- Phishing (91)

Recent Posts

- What is Baiting in Cyber Security?
- 7 Smishing Examples and How to Protect Yourself
- What is Swatting? What to Look for and How to Defend Yourself
- The 2023 Gone Phishing Tournament Results: Everything You Need to Know
- Protect your loved ones from phishing, social engineering and other cyber attacks

Tags

byod CISO Communication tools Covid-19 Scams credential stuffing attacks Cyber Security Awareness cyber security professional Data breaches Data Privacy End user engagement gartner magic quadrant GDPR Training governance Human Risk information security awareness information security program ilse lapointe malware National Cyber Security Awareness Month NCSAM Password phishing Phishing scams phishing simulation ransomware Remote working Security Awareness Framework Security Awareness Training social engineering Social Networks Work from home

Examples of Different Types of Phishing Attacks

Just like everything else on the internet, phishing email attacks have evolved over the years to become more intricate, enticing, and tougher to spot.

To successfully pinpoint and flag suspicious messages in their inbox, all your users must be familiar with phishing emails' different forms.

Phishing Email

Phishing emails still comprise a large portion of the world's yearly slate of devastating data breaches. Phishing emails are designed to appear to come from a legitimate source, like Amazon customer support, a bank, PayPal, or another recognized organization.

Cyber criminals hide their presence in little details like the sender's URL, an email attachment link, etc.

Spear Phishing

This more targeted phishing email attack relies on data that a cyber criminal has previously collected about the victim or the victim's employer. Typically spear phishing emails use urgent and familiar language to encourage the victim to act immediately.

Link Manipulation

Relying on carefully worded phishing emails, this attack includes a link to a popular. This link takes victims to a spoofed version of the popular website, designed to look like the real one, and asks them to confirm or update their account credentials.

Fake Websites

Cyber criminals send phishing emails that include links to fake websites, such as the mobile account login page for a known mail provider, asking the victim to enter their credentials or other information into the fake site's interface.

The malicious website will often leverage a subtle change to a known URL to trick users, such as mail.update.yahoo.com instead of mail.yahoo.com.

CEO Fraud

This example of a phishing attack uses an email address familiar to the victim, like the one belonging to the organization's CEO, Human Resources Manager, or the IT support department. The email urgently asks the victim to act and transfer funds, update employee details, or install a new app on their computer.

Content Injection

Savvy cyber criminals hack a familiar website and include a fake website login page or pop-up that directs website visitors to a fake website.

Session Hijacking

With this advanced phishing attack, criminals gain access to a company web server and steal the confidential information stored on the server.

Malware

In malware attacks, recipients open phishing emails that contain malicious attachments. When clicked, the action installs malicious software on the user's computer or on the company network. These attachments look like valid files. In some cases, they're disguised as funny cat videos, eBooks, PDFs, or animated GIFs.

"Evil Twin" Wi-Fi

This occurs when free Wi-Fi access points are spoofed. Victims unknowingly log into the wrong Wi-Fi hotspot. Wi-Fi access points commonly spoofed include those available in coffee shops, airports, hospitals, shopping malls, public parks, and other public gathering locations.

Mobile Phishing (Smishing)

A fraudulent SMS, social media message, voice mail, or other in-app message asks the recipient to update their account details, change their password, or tell them their account has been violated.

The message includes a link used to steal the victim's personal information or install malware on the mobile device.

Voice Phishing (Vishing)

This scenario occurs when a caller leaves a strongly worded voicemail that urges the recipient to respond immediately and to call another phone number. These voicemails are urgent and convince the victim, for example, that their bank account will be suspended if they don't respond.

Man-In-The-Middle

This sophisticated phishing email attack tricks two people into believing that they're emailing each other. However, the hacker sends fake emails to each person asking them to share information or update confidential corporate information.

Malvertising

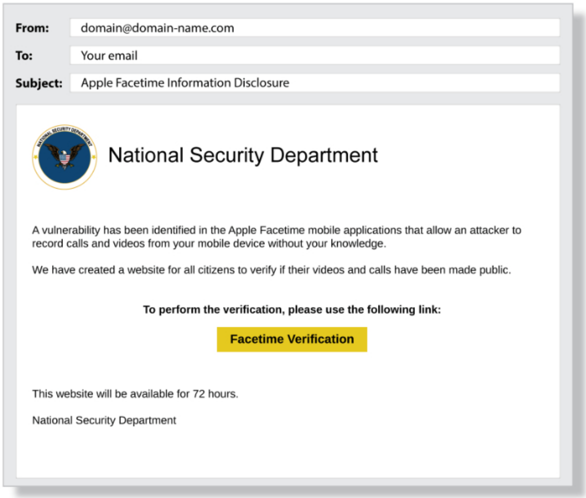
This phishing technique uses online advertisements or pop-ups to compel people to click a valid-looking link that installs malware on their computer.

Real-World Examples of Phishing Email Attacks

One common thread that runs through all types of phishing emails, including the examples below, is the use of social engineering tactics. Like most phishing attacks, social engineering preys on the natural human tendency to trust people and companies.

This leads to many users failing to carefully review phishing email details and automatically trusting the sender's request. Email phishing victims believe they're helping their organizations by transferring funds, updating login details, or providing access to proprietary data.

(example of phishing email)



From:	domain@domain-name.com
To:	Your email
Subject:	Apple Facetime Information Disclosure

National Security Department

A vulnerability has been identified in the Apple Facetime mobile applications that allow an attacker to record calls and videos from your mobile device without your knowledge.

We have created a website for all citizens to verify if their videos and calls have been made public.

To perform the verification, please use the following link:

Facetime Verification

This website will be available for 72 hours.

National Security Department

Make sure your colleagues are aware of these common examples of phishing emails:

Account Deactivation

An email from PayPal arrives telling the victim that their account has been compromised and will be deactivated unless they confirm their credit card details. The link in the phishing email takes the victim to a fake PayPal website, and the stolen credit card information is used to commit further crimes.

Compromised Credit Card

The cyber criminal knows the victim made a recent purchase at Apple, for example, and sends an email disguised to look like it is from Apple customer support. The email tells the victim that their credit card information might have been compromised and to confirm their credit card details to protect their account.

Transfer Funds

An urgent email arrives from the company CEO, who is currently traveling. The email asks the recipient to help the CEO transfer funds to a foreign partner. This phishing email tells the victim that the fund request is urgent and necessary to secure the new partnership.

The victim doesn't hesitate to transfer the funds, believing she is helping both the company and the CEO.

Social Media Request

A Facebook friend request arrives from someone who has the same Facebook friends as you. You don't immediately recognize the person but assume the request is legitimate because of the friends in common.

This new friend then sends you a Facebook message with a link to a video that, when clicked, installs malware on your computer and potentially the company network.

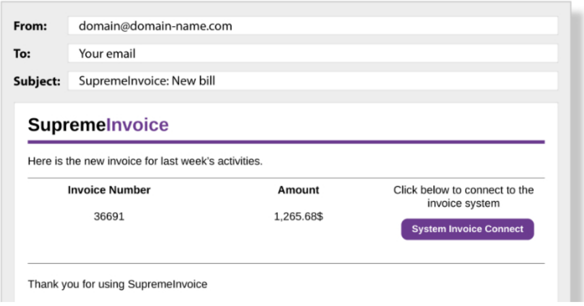
Related reading: Countering The 5 Most Common Social Media Phishing Scams

Fake Google Docs Login

A cyber criminal creates a fake Google Docs login page and then sends a phishing email to trick someone into logging into the faked website. The email might read something like, "We've updated our login credential policy.

Please confirm your account by logging into Google Docs." The sender's email is a faked Google email address, accountupdate@google.org.com.

(example of phishing email)



From:	domain@domain-name.com
To:	Your email
Subject:	SupremeInvoice: New bill

SupremeInvoice

Here is the new invoice for last week's activities.

Invoice Number	Amount	Click below to connect to the invoice system
36691	1,265.68$	System Invoice Connect

Thank you for using SupremeInvoice

Company Tech Support Request

Employees receive an email from corporate IT asking them to install new instant messaging software. The email looks real. However, a spoofed email address is used support@acme.com instead of internalsupport@acme.com.

When employees install the software, ransomware is installed on the company network. These phishing attack examples highlight how easy it is to be tricked by an email. The more familiar people are with how phishing happens, the easier it is to foster a cyber-aware culture.

How to Protect Your Data from Phishing Emails

The examples above highlight how cyber criminals can find so many ways to trick you into giving information. To protect against phishing attacks, people need to be aware of the various types of phishing attacks and know how phishing happens.

The key to prevention is creating a high level of cyber security awareness through training and practice. Phishing simulations are an ideal way to train users how to identify and avoid phishing attacks.

They show users different types of phishing emails and test their powers of discernment. They give employees first-hand experience of phishing scenarios and demonstrate how easy it is to be tricked by what looks like authentic communication through a valid email.

When people return to real life scenarios, they're more likely to carefully review emails, URLs and the context of communication before acting on instinct. Phishing simulations teach people to pause and analyze before automatically clicking "Reply," visiting embedded links, or downloading unsecure attachments.

Follow these five steps to protect against phishing email attacks and build cyber security awareness in your organization:

1. **Educate:** Use security awareness training and phishing microlearnings to educate, train, and change behavior.
2. **Monitor:** Use phishing simulation tools to monitor employee knowledge and identify who in the organization is at high risk for receiving or responding to a phishing attack.
3. **Communicate:** Provide ongoing communications and run campaigns about phishing emails, social engineering, and cyber security.
4. **Incorporate:** Make cyber security awareness campaigns, training, support, education, and project management part of your corporate culture.
5. **Apply:** As end users, apply this knowledge about phishing email attacks in your everyday activities. Be aware of the risks and take the time to assess emails, texts, and websites.

Share: f 𝕏 in t

← Newer
The IRS Won't Call You: Understanding and Avoiding Tax Scams

Older →
Cyber Security In The Education Sector

Cyber Security Training for Employees

Privacy Awareness

Click and Launch

Compliance and Governance

GDPR

Phishing Simulation

Cyber Games

GET STARTED

Free Demo

Request a Quote

Phishing Simulation Trial

Cyber Security Hub

eBook – The Human Fix to Human Risk

Phishing Free Trial

Reports and Guides

Cyber Challenges Demo

STAY CONNECTED

About Terranova Security

Join Our Team

GET IN TOUCH

Contact Us
Customer Support
Cybersafe and Sound Newsletter

Your cyber security awareness newsletter

Business Email*

mfish

Email must be formatted correctly.

SUBMIT

SIGNING UP FOR NEWSLETTERS INDICATES YOU AGREE WITH OUR PRIVACY POLICY.

IF YOU DECIDE THAT YOU NO LONGER WANT TO RECEIVE OUR NEWSLETTERS, YOU CAN UNSUBSCRIBE BY CLICKING THE "UNSUBSCRIBE" LINK, LOCATED AT THE BOTTOM OF EACH NEWSLETTER.

Privacy Policy | Cookie Policy

FORTRA
Terranova Security