www.kirkhamirontech.com

KIRKHAM
IRONTECH

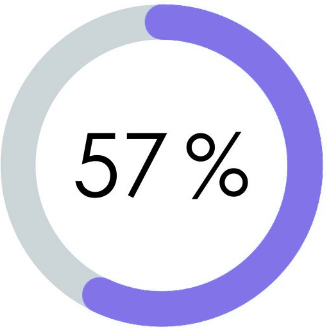
PHISHING ATTACKS

A Proactive Approach to Combating Phishing Attacks

INTRODUCTION

Phishing is one of the most prevalent cyber threats facing businesses today. This type of attack is not only becoming more common but also more sophisticated and successful. In the 2021 State of the Phish Report, 57 percent of the surveyed organizations said they experienced a successful phishing attack in 2020. This figure is up 55 percent from 2019.

Let's take an in-depth look at phishing, a rapidly growing threat that will cost U.S. companies millions of dollars.



> **"57 percent of the surveyed organizations said they experienced a successful phishing attack in 2020."**
>
> – 2021 State of the Phish

What is Phishing?

Phishing is a type of social engineering attack that preys on unsuspecting victims. In its most basic form, phishing involves fraudulent communication from seemingly trustworthy or reputable sources containing messages that provoke a response or action. The scammer can trick victims into revealing sensitive information such as login credentials, granting unauthorized access to a system, or clicking on malicious links or email attachments.

Most phishing attacks are perpetrated via email, although some use social media, text messages, and phone calls. A majority of malware infections get delivered through phishing emails. But regardless of the channel used, the phisher's goal is to make the communication seem genuine and unquestionable. This usually means taking on false but convincing personas such as a fellow employee, customer, IT expert, manager, celebrity, insurer, and so on.

The Different Types of Phishing Scams

While the underlying premise of all phishing attacks is basically the same, the techniques employed can vary widely. Here are the various ways that phishers perpetrate their attacks.

- **Email phishing:** Mass email spraying
- **Spear phishing**: Targeted attacks with personalized messages
- **Whaling/CEO phishing**: Attacks on top officials and executives
- **Vishing**: Phishing via voice calls
- **Smishing**: Phishing via text messages
- **Angler phishing:** The attacker masquerades as a customer service agent through cloned social media profiles or websites.
- **Pharming**: The attacker corrupts a browser's cache so that the domain name system redirects users to a malicious website.
- **Clone phishing:** The attacker creates malicious copies of genuine messages.

How To Spot The Differences Between Real And Fake Emails

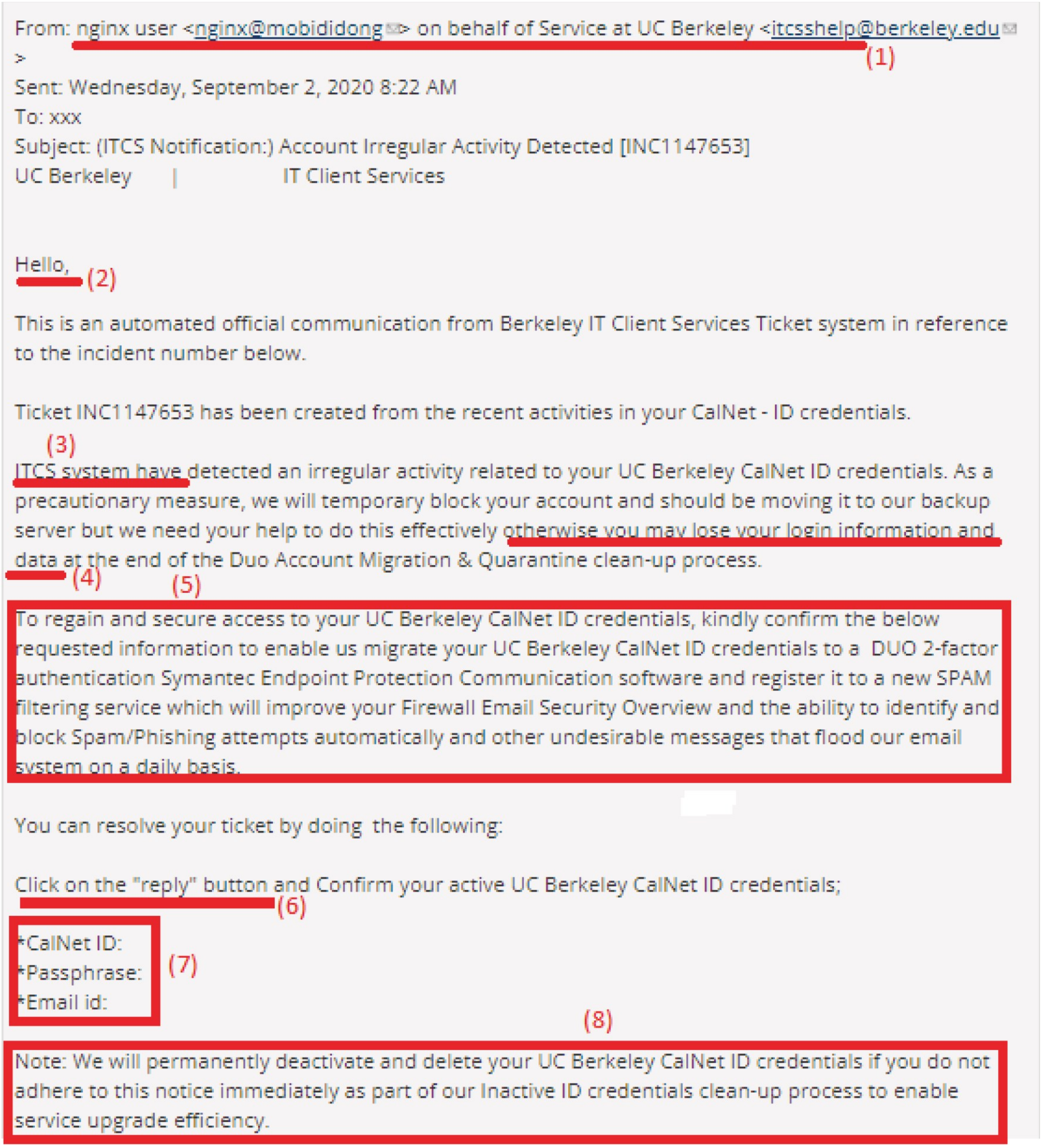
To identify phishing scams, you need first to understand how social engineering works. Social attacks don't prey on just the gullibility of their victims. They also take advantage of easy-to-provoke human emotions such as worry, greed, anxiety, joy, anger, and even grief.

Hackers also use the prevailing social-political climate to conjure convincing lies. For instance, COVID-19 related phishing attacks exploded in 2020. The worst part is that most phishers have the time and patience to craft elaborate scams that can take weeks or even months to orchestrate.

As crafty as phishers are at fabricating emails, you can still see through the deception if you are keen enough and know what to look for. Here are the common telltale signs that give away most phishing emails:

- Unknown sender, sometimes with a vague identity
- Off-brand tone
- Inconsistencies in the sender's branding, identity, email address, or domain names
- Unusual requests, such as downloading a file, installing a program, providing credentials, logging in through the link provided, or forwarding the email
- Generic salutations, such as "dear customer"
- A sense of intense urgency
- Shortened link leading to a suspicious login or download page
- Brief message lacking helpful or detailed information
- Poorly written text, often with grammatical and spelling errors
- Suspicious attachments (strange file types, thumbnails, and file names)
- Bonkers claims such as winning rewards and account suspensions
- Bold threats for not complying with the request

Let's look at this example of a phishing email published in UC Berkeley's Phishing Examples Archives to see how many red flags we can spot:



From: nginx user <nginx@mobididong> on behalf of Service at UC Berkeley <itcsshelp@berkeley.edu>
Sent: Wednesday, September 2, 2020 8:22 AM
To: xxx
Subject: (ITCS Notification:) Account Irregular Activity Detected [INC1147653]
UC Berkeley | IT Client Services

Hello,

This is an automated official communication from Berkeley IT Client Services Ticket system in reference to the incident number below.

Ticket INC1147653 has been created from the recent activities in your CalNet - ID credentials.

ITCS system have detected an irregular activity related to your UC Berkeley CalNet ID credentials. As a precautionary measure, we will temporary block your account and should be moving it to our backup server but we need your help to do this effectively otherwise you may lose your login information and data at the end of the Duo Account Migration & Quarantine clean-up process.

To regain and secure access to your UC Berkeley CalNet ID credentials, kindly confirm the below requested information to enable us migrate your UC Berkeley CalNet ID credentials to a DUO 2-factor authentication Symantec Endpoint Protection Communication software and register it to a new SPAM filtering service which will improve your Firewall Email Security Overview and the ability to identify and block Spam/Phishing attempts automatically and other undesirable messages that flood our email system on a daily basis.

You can resolve your ticket by doing the following:

Click on the "reply" button and Confirm your active UC Berkeley CalNet ID credentials;

*CalNet ID:
*Passphrase:
*Email id:

Note: We will permanently deactivate and delete your UC Berkeley CalNet ID credentials if you do not adhere to this notice immediately as part of our Inactive ID credentials clean-up process to enable service upgrade efficiency.

1. An ambiguous identity that doesn't disclose the sender's name
2. Generic greeting, not addressing anyone in particular
3. Grammatical errors here and there
4. Threat/consequence of non-compliance
5. Over explained jargon-filled fluff that makes little sense
6. Unusual requests; automated messages usually don't take replies
7. No legitimate company or tech support team will ever ask you for login credentials
8. More threats and a sense of urgency

The Rise Of More Sophisticated Threats

Not all phishing attempts are as simple and easy to identify as the example we've used above. Some are way more intricate. The sophistication of any phishing attack depends on how much the attacker already knows about the target victim. Unfortunately, cybercriminals can quickly get their hands on enough personal information from online forums, press, webchats, social media, and spyware to forge foolproof scams.

Plus, phishers are becoming better at selling deception. Most phishing emails try to redirect victims to a fake login page that resembles a genuine website — for instance, a fake Gmail login page. The victim then enters their actual login credentials into the fake form, which the trickster harvests and uses to compromise the victim's real account.

These malicious sites are so well designed that most people can't tell them apart from the real thing. Some are so good that they even outwit the AI-based web crawlers that hunt look alike websites. In most cases, it's the URL mismatch that gives phishing sites away.

Phishing-as-a-Service is another new trend fueling the growth of phishing attacks. This underground cottage industry makes phishing toolkits readily available to scammers, lowering the technical entry point for complex phishing attacks.

How to Protect Your Business Against Phishing Attacks

> “... human element accounts for the majority of data breach incidents.”
>
> – Verizon

The most effective defense against phishing attacks is to quickly train employees to recognize and respond appropriately to phishing advances. No matter how compelling, personalized, or well-crafted a phishing email gets, it always has a tell. This tell could be the unidentifiable sender, the unusual URL, the odd request, timing, or the message’s tone. Teach your employees to spot even the most subtle red flags and report suspicious emails to the security team.

In addition to phishing awareness training, urge all staff members not to click on links or attachments from unknown senders or give in to any demands for sensitive information. Also, keep in mind that the human element accounts for the majority of data breach incidents. So, take a holistic employee training approach that covers all possible threats facing your organization, not just phishing. A good grasp of the cyber threat landscape fully prepares your organization for whatever cybercriminals can throw its way.

Besides comprehensive employee training, here are a few more preventive measures you can take to wade off scammers:

- Install anti-phishing tools on all endpoints to detect and block malicious sites.
- Enable spam filters on browsers and email clients that quarantine and check suspicious emails before reaching the inbox.
- Install robust anti-malware systems to stop malicious code from running.

- Use multi-factor authentication (MFA) on all user accounts.
- Take a Zero Trust security approach.
- Install impenetrable firewalls all around the corporate network.

Phishing is not a threat to take lightly. Luckily, you can quickly mitigate most social engineering risks with the proper knowledge, expertise, and tools. You only need a high level of threat awareness and preparedness, a robust security infrastructure, and everyone pulling in the same direction.

However, managing cybersecurity can be challenging and confusing, especially when you don't know where to start. But don't worry, you can count on us to do all the heavy lifting on your behalf. Don't hesitate to contact us if you need expert assistance in reinforcing your cybersecurity defenses.

Contact Us

www.kirkhamirontech.com

479-434-1400

3111 Old Greenwood Road
Fort Smith, AR 72903