Phishing Prevention

112003151 – Adwait Vipra
112003158 – Shyam Aradhye
112007014 – Ved Bilaskar

Phishing attack definition refers to the fraudulent use of electronic communications to deceive and take advantage of unsuspecting internet users. They are cleverly designed to gain sensitive, confidential data such as credit card information, network credentials, usernames, passwords, and more. Adversaries use social engineering techniques to trick users into performing specific actions. These include clicking a malicious link or attachment or divulging confidential information willfully due to ignorance.

Here's How Phishing Works

In a typical case, you'll receive an email that appears to come from a reputable company that you recognize and do business with, such as your financial institution. In some cases, the email may appear to come from a government agency, including one of the federal financial institution regulatory agencies.

The email will probably warn you of a serious problem that requires your immediate attention. It may use phrases, such as "Immediate attention required," or "Please contact us immediately about your account." The email will then encourage you to click on a button to go to the institution's Website.

In a phishing scam, you could be redirected to a phony Website that may look exactly like the real thing. Sometimes, in fact, it may be the company's actual Website. In those cases, a pop-up window will quickly appear for the purpose of harvesting your financial information.

In either case, you may be asked to update your account information or to provide information for verification purposes: your Social Security number, your account number, your password, or the information you use to verify your identity when speaking to a real financial institution, such as your mother's maiden name or your place of birth.

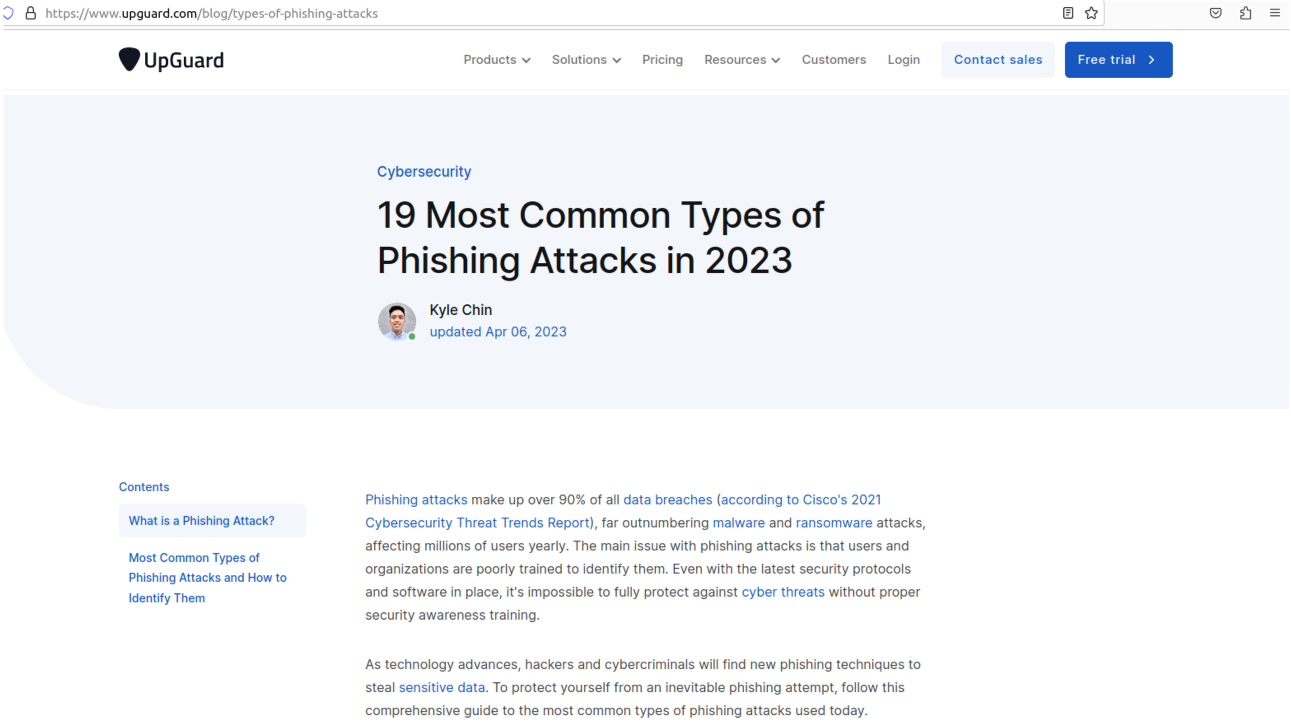
If you provide the requested information, you may find yourself the victim of identity theft.

Phishing prevention measures :

1. Keep updated with the latest ways

New phishing attack methods are being developed all the time, but they share commonalities that can be identified if you know what to look for. There are many sites online that will keep you informed of the latest phishing attacks and their key identifiers. The earlier you find out about the latest attack methods and share them with your users through regular security awareness training, the more likely you are to avoid a potential attack.

Eg :



Cybersecurity

19 Most Common Types of Phishing Attacks in 2023

Kyle Chin
updated Apr 06, 2023

Contents

What is a Phishing Attack?

Most Common Types of Phishing Attacks and How to Identify Them

Phishing attacks make up over 90% of all data breaches (according to Cisco's 2021 Cybersecurity Threat Trends Report), far outnumbering malware and ransomware attacks, affecting millions of users yearly. The main issue with phishing attacks is that users and organizations are poorly trained to identify them. Even with the latest security protocols and software in place, it's impossible to fully protect against cyber threats without proper security awareness training.

As technology advances, hackers and cybercriminals will find new phishing techniques to steal sensitive data. To protect yourself from an inevitable phishing attempt, follow this comprehensive guide to the most common types of phishing attacks used today.

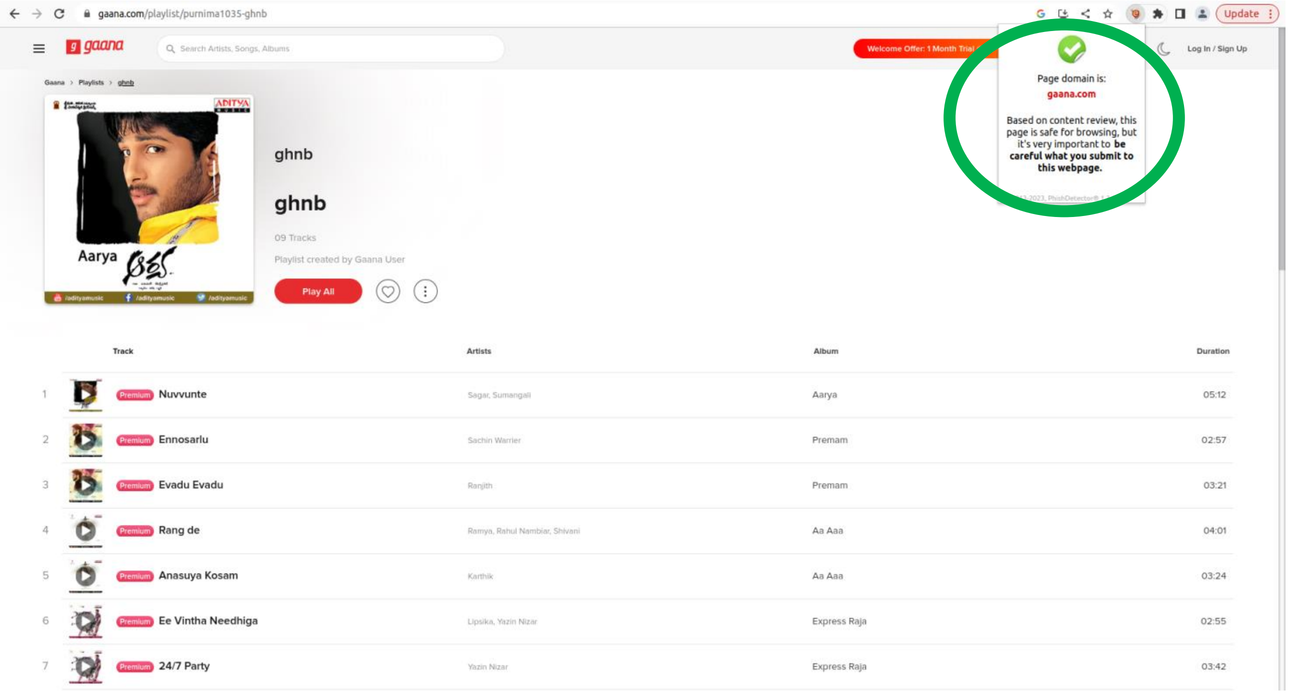
2. Don’t click on that link

It’s generally not advisable to click on a link in an email or instant message, even if you know the sender. The bare minimum you should be doing is hovering over the link to see if the destination is the correct one. Some phishing attacks are fairly sophisticated, and the destination URL can look like a carbon copy of the genuine site, set up to record keystrokes or steal login/credit card information. If it’s possible for you to go straight to the site through your search engine, rather than click on the link, then you should do so.

3. Get free anti-phishing add-ons

Most browsers nowadays will enable you to download add-ons that spot the signs of a malicious website or alert you about known phishing sites. They are usually completely free so there’s no reason not to have this installed on every device in your organization.

eg : Chrome extension – PhishDetector


gaana.com/playlist/purnima1035-ghnb
Update
gaana
Search Artists, Songs, Albums
Welcome Offer: 1 Month Trial
Log In / Sign Up
Gaana > Playlists > ghnb
Aarya
/adityamusic
Play All

Page domain is:
gaana.com

Based on content review, this page is safe for browsing, but it's very important to **be careful what you submit to this webpage.**

ghnb

ghnb

09 Tracks

Playlist created by Gaana User

	Track	Artists	Album	Duration
1	Premium Nuvvunte	Sagar, Sumangali	Aarya	05:12
2	Premium Ennosarlu	Sachin Warrier	Premam	02:57
3	Premium Evadu Evadu	Ranjith	Premam	03:21
4	Premium Rang de	Ramya, Rahul Nambiar, Shivani	Aa Aaa	04:01
5	Premium Anasuya Kosam	Karthik	Aa Aaa	03:24
6	Premium Ee Vintha Needhiga	Lipsika, Yazin Nizar	Express Raja	02:55
7	Premium 24/7 Party	Yazin Nizar	Express Raja	03:42

4. Don't give your information to an unsecured site

If the URL of the website doesn't start with "https", or you cannot see a closed padlock icon next to the URL, do not enter any sensitive information or download files from that site. Sites without security certificates may not be intended for phishing scams, but it's better to be safe than sorry.

5. Rotate passwords regularly

If you've got online accounts, you should get into the habit of regularly rotating your passwords so that you prevent an attacker from gaining unlimited access. Your accounts may have been compromised without you knowing, so adding that extra layer of protection through password rotation can prevent ongoing attacks and lock out potential attackers.

6. Don't ignore those updates

Receiving numerous update messages can be frustrating, and it can be tempting to put them off or ignore them altogether. Don't do this. Security patches and updates are released for a reason, most commonly to keep up to date with modern cyber-attack methods by patching holes in security. If you don't update your browser, you could be at risk of phishing attacks through known vulnerabilities that could have been easily avoided.

7. Install firewalls

Firewalls are an effective way to prevent external attacks, acting as a shield between your computer and an attacker. Both desktop firewalls and network firewalls, when used together, can bolster your security and reduce the chances of a hacker infiltrating your environment.

8. Don’t be tempted by those pop-ups

Pop-ups aren’t just irritating; they are often linked to malware as part of attempted phishing attacks. Most browsers now allow you to download and install free ad-blocker software that will automatically block most of the malicious pop-ups. If one does manage to evade the ad-blocker though, don’t be tempted to click! Occasionally pop-ups will try and deceive you with where the “Close” button is, so always try and look for an “x” in one of the corners.