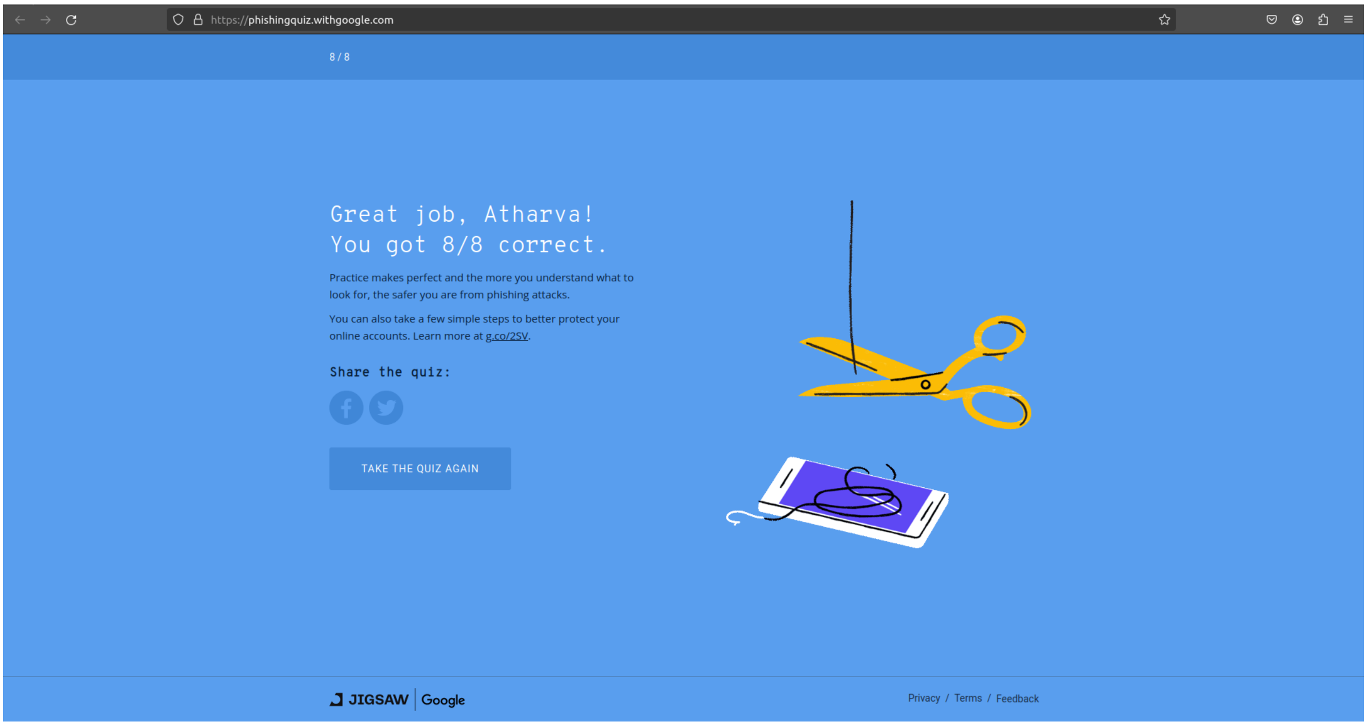
Phishing Project

Task 1



https://phishingquiz.withgoogle.com
8 / 8

Great job, Atharva!
You got 8/8 correct.

Practice makes perfect and the more you understand what to look for, the safer you are from phishing attacks.

You can also take a few simple steps to better protect your online accounts. Learn more at g.co/2SV.

Share the quiz:

TAKE THE QUIZ AGAIN
JIGSAW Google
Privacy / Terms / Feedback

This task gave us some examples and techniques on how to identify a phishong site.

Task 2

What is Phishing ?

```
Phishing is a form of social engineering and scam where attackers decieve
people into revealing sensitive information or installing malware such as
ransomware.
```

Types of phishing

Email Phishing

```
Phishing assaults, which are frequently sent via email spam, aim to deceive
people into divulging personal information or login credentials. The
majority of attacks are classified as "bulk attacks" since they are
distributed in large quantities to a large audience without any specific
target.Financial organizations, email and cloud productivity providers, and
streaming services are the typical targets.
```

Spear Phishing

```
Spear phishing is a targeted phishing attack that uses personalized emails
to trick a specific individual or organization into believing they are
legitimate. It often utilizes personal information about the target to
increase the chances of success.These attacks often target executives or
those in financial departments with access to sensitive financial data and
services.
```

Vishing

```
Voice phishing, or vishing, is an attack technique in which attackers
utilize automated phone calls to a large number of victims.The assailants
claim to be employed by a respectable bank or company. Subsequently, the
victim is requested to enter their sensitive details.
```

Smishing

```
Phishing attacks that use text messages from a smartphone or cell phone to
send a bait message are known as SMS phishing, or smishing.Typically, the
attacker asks the victim to click on a website, dial a telephone, or send
an email to an address they have provided. Subsequently, they can be
requested for confidential data, including login credentials for more
websites.
```

Pharming

```
Pharming is a cyberattack intended to redirect a website's traffic to
another, fake site by installing a malicious program on the victims
computer thus having access to it. Pharming can be conducted either by
changing the hosts file on a victim's computer or by exploitation of a
vulnerability in DNS server software.
```

Other common phishibg techniques are :

```
CLONE PHISING : A clone phishing attack involves a hacker making an
identical copy of a message the recipient already received. They may
include something like “resending this” and put a malicious link in the
email.

WHALING : A whaling attack is a phishing attack that targets a senior
executive. These individuals often have deep access to sensitive areas of
the network, so a successful attack can result in access to valuable info.
```

```
QUISHING : Quishing, or QR phishing, is a type of cybersecurity threat in
which attackers create QR codes to redirect victims into visiting or
downloading malicious content.

WEBSITE SPOOFING : With website spoofing, a hacker creates a fake website
that looks legitimate. When you use the site to log in to an account, your
info is collected by the attacker.
```

Psychological Tactics

```
Some of the psychological tactics used for phishing are:

1. URGENCY AND FEAR:
    Phishers often create a sense of urgency or fear to prompt immediate
action.They can say that money is in danger, an account is hacked, or the
victim will face legal repercussions if they don't act right away.

2. CURIOSITY:
    Phishing emails and messages can attract attention with attention-
grabbing subject lines or content. Attackers take use of victims' innate
curiosity by tricking them into clicking links or opening attachments.

3. AUTHORITY AND TRUST:
    Phishers may pose as representatives of a reliable service provider,
the IT department, or the security division. They hope to persuade victims
to follow orders without question by asserting their authority.

4. MIMICKING
    Email spoofing is a technique used by phishers to pretend that mails
are from reputable sources. This can involve imitating official
communication by using identical email accounts, logos, and layout.

5. REWARDS
    Phishing attacks might use exclusive offers, awards, or prizes to trick
victims into divulging personal information. The possibility of obtaining
something appealing can impair judgment.

Other tatics include Obfuscation,Social Engineering, Personalization etc.
```

Real-Life Examples

```
Here are some of the real life examples of phishing:-

1.Facebook and Google:
    A lengthy phishing campaign defrauded Facebook and Google of $100
million between 2013 and 2015. The phisher used the fact that Quanta, a
Taiwan-based business, was a vendor for both organizations. The impostor
```

```
company received several bogus invoices from the attacker, which were paid
for by Google and Facebook.

2.Crelan Bank
    The business email compromise (BEC) scam that targeted Crelan Bank in
Belgium cost the organization roughly $75.8 million. In this kind of
attack, a phisher gains access to a high-ranking executive's account at a
corporation and instructs staff members to move funds to an account under
the attacker's control.

3.FACC
    FACC, an Austrian manufacturer of aerospace parts, also lost a
significant amount of money to a BEC scam. In 2016, the organization
announced the attack and revealed that a phisher posing as the company’s
CEO instructed an employee in the accounting department to send $61 million
to an attacker-controlled bank account.
```

Task 3

```
Phishing attacks can have severe consequences for both individual victims
and organizations, ranging from financial losses to reputational damage and
legal liabilities.
```

Financial Impacts

```
1.Financial Losses:
    If phishing attack victims unintentionally provide private information—
such as login credentials, credit card numbers, or bank account details—
they could incur immediate financial damages. Hackers could then use this
data for theft or fraudulent transactions.

2.Fraudulent Transactions:
    Attacks using phishing techniques frequently result in illicit
transactions that drain victims' accounts of money. The financial damage
may be exacerbated in certain instances where victims fail to discover
these transactions right away.

3.Cost of Remediation:
    Businesses that are attacked by phishers frequently have to pay a high
price for restoration work. This entails carrying out forensic
investigations, putting security updates into place, and offering impacted
parties credit monitoring services.
```

Reputational Impacts

```
1.Loss of Trust:
    Businesses who don't defend against phishing attempts run the danger of
losing the confidence of their partners, clients, and consumers. A well-
publicized breach has the potential to damage a business's brand and reduce
customers' trust in its security measures.

2.Brand Damage:
    Businesses who don't defend against phishing attempts run the danger of
losing the confidence of their partners, clients, and consumers. A well-
publicized breach has the potential to damage a business's brand and reduce
customers' trust in its security measures.

3.Customer Churn:
    Customers may decide to cut their connections with a compromised
company after a phishing assault because they are worried about their
security and privacy. In the long run, this can result in higher client
attrition and lower revenue.
```

Legal Impacts

```
1.Regulatory Fines:
    Organizations that violate data protection rules like the CCPA, GDPR,
or HIPAA may be subject to fines and penalties from the government. This is
because they are failing to effectively protect sensitive information.
These penalties might add significantly to the financial damage caused by a
phishing assault.

2.Lawsuits:
    Phishing attack victims may file a lawsuit against the company that
allowed the breach, claiming that they were careless in protecting their
personal data. Class-action lawsuits have the potential to yield large
settlements and legal costs.

3.Reputation in Legal and Regulatory Circles:
    Businesses who lose data due to phishing attempts risk harm to their
reputation in legal and regulatory circles. Regulators may become more
suspicious of this, which could make it harder to get the required
permissions or clearances.

Some Indian laws regarding cybersecurity is:

    1.Information Technology Act, 2000 (IT Act)

    2.Data Protection Bill

    3.The Indian Penal Code (IPC)

    4.The Payment and Settlement Systems Act, 2007
```

Long-term Consequences

```
1. Identity Theft:
    The theft of personally identifiable information (PII), which can be
used to commit identity theft, is a common component of phishing assaults.
Long-term effects for victims could include ruined credit ratings, trouble
getting loans or credit cards, and trouble closing fraudulent accounts.

2.Data Breaches:
    Phishing attacks have the potential to act as gateways for more
significant data breaches, revealing private data including corporate
secrets, financial details, and intellectual property. A data breach may
have long-term repercussions such as decreased market share, litigation,
and loss of competitive advantage.

3.Legal Liability:
    Businesses who don't take appropriate precautions to avoid phishing
attacks could be held legally responsible for violating data privacy
regulations, failing to protect client information, or defaulting on
contracts. Regulatory bodies' lawsuits, settlements, and fines can have a
long-term negative financial and legal impact on the organization.

4.Credit Score Damage:
    A phishing attack may have long-term effects on a person's credit score
if it leads to identity theft or illicit financial transactions in their
name. It could take some time and effort to resolve problems relating to
fraudulent accounts or transactions, which could affect the person's future
ability to get credit cards, loans, or mortgages.

5.Psychological Impact:
    Phishing assaults can leave their victims with severe worry, anxiety,
and emotional discomfort, especially if they lose money or find it
difficult to deal with the fallout. Being the target of cybercriminals can
have a long-term psychological effect on someone's security and general
well-being.
```

Task 4

Task 5

```
Some ways to prevent phishing:

1.Educational Campaigns:
    The dissemination of knowledge regarding phishing assaults is mostly
dependent on educational programs. Businesses such as KnowBe4 focus on
offering training modules and simulated phishing attacks to teach consumers
how to spot and steer clear of phishing efforts.

2.Email Authentication Protocols:
    By putting email authentication methods like DMARC (Domain-based
Message Authentication, Reporting, and Conformance), DKIM (DomainKeys
Identified Mail), and SPF (Sender Policy Framework) into practice, one can
lessen the likelihood of phishing attacks by confirming the legitimacy of
emails.

3.Anti-Phishing Software:
    AI-powered anti-phishing solutions are provided by startups like
IronScales, which examine email trends and identify irregularities
suggestive of phishing attempts. In order to offer real-time protection,
these solutions frequently integrate with already-in-use email services.

4.Browser Extensions:
    Browser extensions like Netcraft and MetaCert can help users identify
and block phishing websites by analyzing URLs in real-time and providing
warnings when visiting suspicious sites.

5.Two-Factor Authentication (2FA):
    By forcing users to give two forms of authentication before accessing
their accounts, 2FA adds an extra layer of security and makes it more
difficult for attackers to obtain unauthorized access through phishing.

6.Open-Source Solutions:
    Organizations can utilize open-source technologies such as Gophish to
train staff and assess their susceptibility to phishing assaults
internally. These programs also offer phishing simulation and awareness
training platforms.
```