# Phishing Awareness:

## Protect Against Phishing Threats

Phishing attacks are a common type of cybercrime that aims to trick people into people into revealing sensitive information or installing malware.

**by Abuhuraira Abubakar**


# What is Phishing?

## 1 Deceptive Practice

Phishing is a fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity.

## 2 Email Spoofing

Scammers often use fake emails or websites to trick individuals into providing personal or financial data.

# Common Types of Phishing Attacks

## Pharming

Reroutes website traffic to to fraudulent sites that appear legitimate.

## Spear Phishing

Targets specific individuals or organizations with personalized messages.

## Whaling

Directs attacks at high-profile targets within businesses, such as executives.


# Signs of a Phishing Email

1 **Urgent Requests**

Phishing emails often create a sense of urgency to prompt immediate action.

2 **Spelling Errors**

Grammatical mistakes or typos can reveal the illegitimacy of an email.

# How to Avoid Falling for Phishing Scams

### 1 Verify Senders

Always double-check check the sender's email address before before responding to to requests.

### 2 Hover over Links

Hovering over links can reveal the true destination, helping to to identify fake URLs. URLs.

### 3 Think Before Clicking

Avoid clicking on suspicious links or downloading attachments from unknown sources.

# Importance of Strong Passwords

1

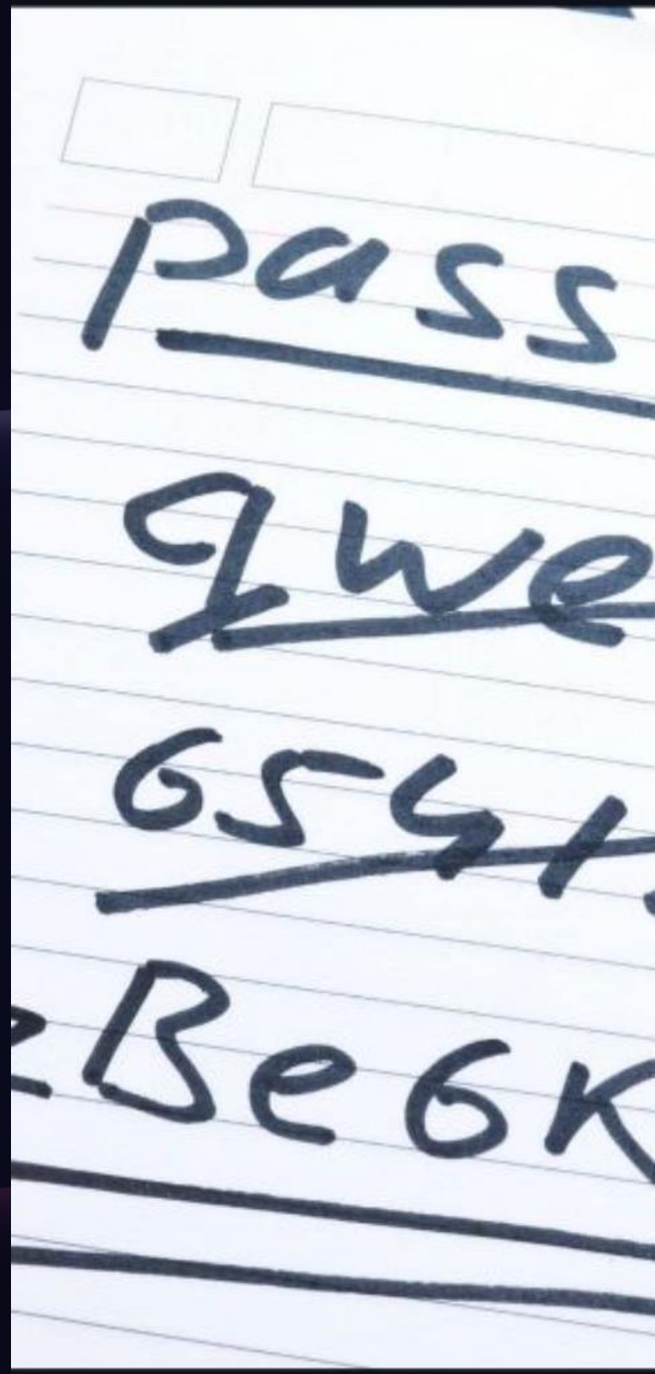
## Complexity

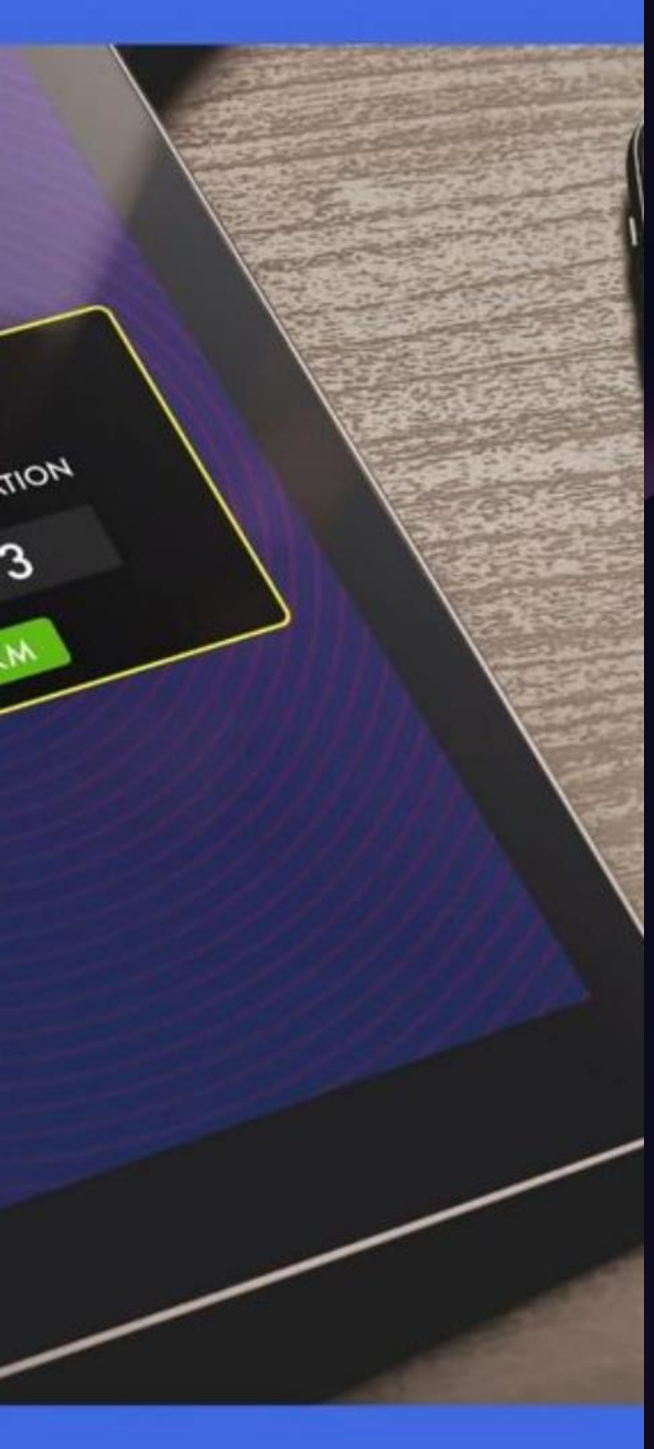
Create passwords with a mix of upper and lower case letters, numbers, and symbols.

2

## Unique Passwords

Use distinct passwords for different accounts to prevent centralized breaches.





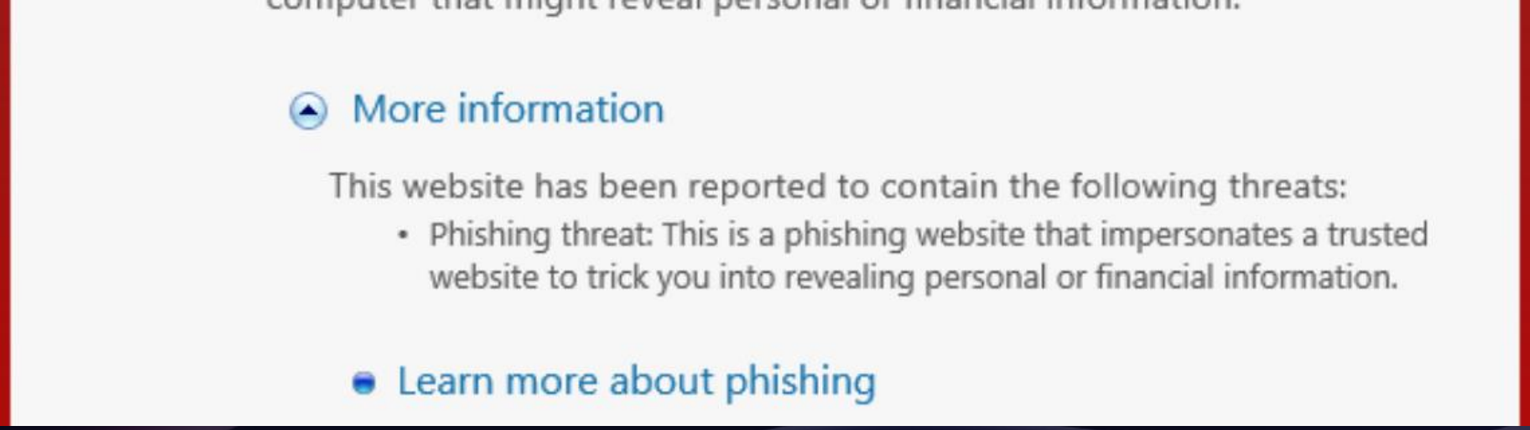
# Two-Factor Authentication

## Extra Layer of Security

Two-factor authentication adds an additional step to the login process, enhancing security.

## Secure Sign-Ins

Requires a secondary code or prompt sent prompt sent to a trusted device for account access.




# Reporting Phishing Attempts

1

## Internal Policies

Organizations should have clear clear protocols for reporting suspected phishing attempts.

2

## Employee Training

Offer training to recognize and report potential phishing threats. threats.

3

## IT Response

Organizations need to have measures in place to respond swiftly to reported incidents.

# Case Studies of Successful Phishing Attacks

| Target | Data Compromised | Consequences |
| --- | --- | --- |
| Company A | Employee IDs, SSNs | Financial Loss, Reputational Damage |
| Organization B | Customer Personal Info | Regulatory Penalties |

# Conclusion and Next Steps

1 **Stay Informed**

Regularly update knowledge about phishing techniques and cybersecurity best practices.

2 **Security Measures**

Implement robust security measures to mitigate the risks posed by phishing attacks.