Cybersecurity Awareness Month
Secure Our World Together

Understand the Risks and Consequences

1 Be a Password Pro

- Create strong, unique passwords for all accounts
- Use a company-approved password manager
- Action: Set up your password manager today

2 Double Your Defenses

- Enable multi-factor authentication (MFA) on all accounts
- Use company-provided MFA tools
- Action: Turn on MFA for all your work accounts now

3 Spot and Stop Phishing

- Learn to identify suspicious emails and links
- Report potential phishing attempts to IT immediately
- Action: Take a phishing awareness quiz this week

4 Stay Up-to-Date

- Install software updates promptly
- Allow automatic updates when possible
- Action: Check for updates on your devices right now

Avoid Dark Web Breaches

Understand the Risks and Consequences

What Happens to Unsecured Data?

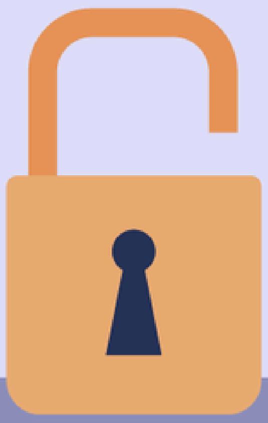
Personal information can be stolen through phishing, data breaches, or malware.
Stolen data is often sold on dark web marketplaces.

Types of Data at Risk?

- Login credentials
- Social Security numbers
- Credit card information
- Medical records
- Company intellectual property

Dark Web Data Market

- Approximately 2.5 million daily visitors as of 2023
- An estimated 57% of content is illegal
- Accounts for only about 5% of the total internet



Consequences of Data Breaches

- Identity theft
- Financial loss
- Reputational damage
- Legal and regulatory penalties for the company

How to Protect Yourself

- Use strong, unique passwords for all accounts
- Enable multi-factor authentication
- Be cautious of phishing attempts
- Keep software and systems updated
- Use encryption for sensitive data

Take Action if Breached

- Change passwords immediately
- Monitor your accounts for unusual activity
- Place a fraud alert on your credit reports
- Report the incident to your IT department

Phishing & Email Fraud Stats

1

There has been a **36.6% increase in phishing** emails in the first three months of 2024 compared to the previous quarter. 2024 Phishing Threat Trends Report.

2

94% of organizations surveyed experienced phishing attacks in 2023.

3

The volume of phishing emails has **increased by 1,265%** since ChatGPT was released in November 2022.

4

Sunday is the favored day for phishing emails, accounting for 22% of attacks, closely followed by Friday at 19%.

5

20.2% of phishing emails employ technical measures to evade Microsoft 365 and secure email gateway detection.

6

QR code phishing or **"quishing" has skyrocketed,** increasing from 0.8% of phishing email payloads in 2021 to 10.8% in the past three months of 2024.

5 COMMON TYPES OF PHISHING

1

Spear Phishing

A highly targeted form of phishing, this attack vector is used to send emails to specific and well-researched targets, while purporting to be from a trusted sender.

2

CEO Fraud

A social engineering technique where an attacker impersonates the CEO/ a senior figure, to trick internal staff into sending payments or sharing sensitive data.

3

Vishing

Also known as 'Voice Phishing', an attacker will make phones calls while pretending to be from a reputable company, in order to induce individuals to reveal personal information.

4

Smishing

Also known as 'SMS Phishing', an attacker will send text messages purporting to be from reputable companies, in order to trick people into giving away personal information.

5

Email Phishing

The fraudulent practice of sending emails purporting to be from reputable companies, often for financial gain or to encourage individual to reveal personal information.

6 Tips for Staying Cyber Safe

Follow these tips to stay safe online whilst at work or at home.

1 Use a strong password

Your passwords should be strong in order to make it more difficult for an attacker to hack or guess them. Using 3 random words is a good way to create a strong, unique password that you will remember.

2 Turn on 2FA

Two-factor authentication (2FA) helps to stop hackers from getting into your accounts, even if they have your password. It does this by asking for more information to prove your identity, such as a code that gets sent to your phone.

3 Update your devices

Out-of-date software, apps, and operating systems contain weaknesses, making them easier to hack. Enable automatic updates for devices and software where possible, and remember to manually update when this is not possible (you'll often get a reminder).

4 Back up your data

Backing up means creating a copy of your information and saving it to another device or to cloud storage (online). Backing up regularly means you will always have a recent version of your information saved. This will help you recover quicker if your data is lost or stolen.

5 Look out for phishing

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. Be suspicious of emails that ask for sensitive information, especially when coming from an unknown source.

6 Don't re-use passwords

If a hacker gets into your email, they could reset your other account passwords and access information you have saved about yourself or your business. Your email password should be different to all your other passwords. Try saving your password to your web browser (such as Chrome, Safari or Edge) for easy remembering.

Information taken from the National Cyber Security Centre (NCSC)

7 SIGNS YOU'RE BEING PHISHED!

Some common warning signs of a potential phishing email.

The email is poorly written

Although scammers can accidentally fall short in the grammar department, these 'mistakes' aren't always unintentional. Errors can be purposefully included in order to limit interaction with only the more 'observant'.

It contains unsolicited attachments

Typically, authentic institutions don't randomly send emails with attachments, especially when there is no previous relationship involved. If in doubt, contact the legitimate company by searching for their website.

It requests sensitive information

Emails that ask you to send sensitive info, such as banking details, tax scores or login credentials, are seriously phishy. You should search online and contact the organisation directly - not the sender.

There's urgency involved

Some scammers try to inflict urgency in their emails - often with threats of account expiration, fines or even prize giveaways - to encourage us to make rash decisions without proper thought.

It sounds to good to be true

Scammers often include 'limited' and 'unmissable' prize giveaways in their phishing emails in an attempt to blur our safety glasses. How does the old adage go? "If it sounds to good to be true...".

It doesn't address you by name

Many phishing scams are sent in their masses, with none (or limited) personalisation involved.

The email address looks altered

Scammers can make their email address look legitimate by including the company name within the structure of their email (e.g john@paypal123.com). Hover over links to make sure they don't look altered.