usecure

SHINING A LIGHT ON THE DARK WEB

Learn about the state of stolen employee credentials on the dark web.



THE DARK WEB ISN'T JUST FOR THE FEW

Two million active users connect to the Dark Web every day and about 60% of the information on the Dark Web could potentially harm organisations.





DARK WEB ACTIVITY IS BOOMING

Overall, the volume of compromised user data freely posted on the dark web rose by almost 30 percent in 2023, compared to the previous year.

Source: Kaspersky

4 COMMON ITEMS FOUND ON THE DARK WEB

1. Documents, like passports (43%)
2. Financial data (39%)
3. Account data (12%)
4. Emails and passwords (6%)

Source: NordVPN





EMAILS CAN BE BOUGHT IN BIG QAUNTITIES

Cyber criminals often purchase batches of email addresses which are then used to launch broad attacks against users..

usecure

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.

usecure

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.

usecure

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.



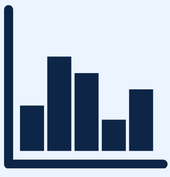
2 Turn on 2FA

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)

usecure

4 REASONS TO DELIVER SECURITY AWARENESS TRAINING

Four key statistics.

Security-related incidents are reduced by 70% when businesses invest in cyber security awareness training.





A modest investment in training has a **72% chance of reducing the business impact** of a cyber attack.

According to Ponemon, even the least effective **training programs have a 7-fold ROI**.





93% of cyber security professionals agree that **humans and tech need to work together** to detect and respond to threats, like phishing.

Sources:
Aberdeen Group Ironscales
CSO Online

SECURITY AWARENESS TRAINING

OLD-SCHOOL

VS

NEW-SCHOOL

How outdated **classroom-style** compares with modern **computer-based** SAT.

Classroom/ PPT	Computer-Based
Tick-box driven, rushed & crammed into single sessions.	Human-focused, designed to improve behaviour & culture.
Boring, unengaging and difficult to retain key info.	Bite-sized training, with interactive & engaging content.
Irregular training (e.g.once-per-year) with outdated content that misses out key threats.	Ongoing and regular learning, with up-to-date content that addresses modern and relevant threats.
Difficult to measure progress, successes, failures & ROI.	Easily report on progress, ROI & demonstrate compliance efforts.