KnowBe4.com
Human error. Conquered.

Which email addresses are exposed on the internet and are a target for phishing attacks?

Your end-users are the weak link in your network security. Today, your employees are frequently exposed to advanced phishing attacks. Trend Micro recently reported that 91% of successful data breaches start with a phishing attack.

Are you aware that many of the email addresses of your organization are exposed on the Internet and easy to find for cybercriminals? With these addresses they can launch spear-phishing attacks on your organization. This type of attack is very hard to defend against, unless your users get next-generation security awareness training.

IT Security specialists call it your 'phishing attack surface'

The more email addresses that are exposed, the bigger your attack footprint is, and the higher the risk. It's often a surprise how many of your addresses are actually out there, whose, and where they were found. Attackers use these email addresses to send targeted attacks to your organization's employees, often using personal information they have found on social media like Facebook or LinkedIn.

> ***"Social Engineering is information security's weakest link."***
> ***– Kevin Mitnick. 'The World's Most Wanted Hacker', Chief Hacking Officer, KnowBe4***

What Exactly Is An Email Exposure Check?

KnowBe4 does a 'deep search' on the Internet, and finds as many email addresses of your domain name as possible. We look deep into websites, and look into Word, Excel and PDF files that are out on the net. The result is an email sent to you, with the list of email addresses that are out there, and also where we found them. It has happened that the credentials of an employee show up on a crime or porn site. Once you know where these addresses are found, you can take defensive action.

Sign Up For Your Free Email Exposure Check

Find out now which of your email addresses are exposed. The Email Exposure Check (EEC) is a one-time free service. KnowBe4 customers with a Gold package get an EEC sent to them regularly so they can address the issues that are found. The number is usually higher than you think. We need a valid email address from the domain of your own organization. That means Gmail, AOL, Yahoo or any other ISP are not eligible for an EEC.

Who Are We?

KnowBe4 helps you keep your network secure with Kevin Mitnick Security Awareness Training ™. You are able to send simulated phishing attacks before and after the training. Created 'by admins for admins', very little time is needed with visible proof the training works.

It's easy to understand why Security Awareness Training now is an essential part of your defense-in-depth. KnowBe4 is the market leading on-demand Security Awareness Training provider that enables organizations to quickly solve the increasingly urgent security problem of social engineering.

With a unique, world-class security awareness training product, KnowBe4 provides self-service enrollment, and both pre-and post-training audits of the percentage of end-users that is phish-prone. KnowBe4 also provides an ongoing, regular security audit to keep employees on their toes, and provides instant remedial online training in case an employee falls for a simulated phishing attack.

The security awareness training project leader at every KnowBe4 customer gets access to user provisioning, and comprehensive pre- and post-training reporting. Every end-user gets engaging and effective 30-40 minute training and after being trained can receive ongoing testing. Business leaders get the insight they need to maximize training ROI and track security compliance.

KnowBe4, LLC | 601 Cleveland Street, Suite 230, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: sales@KnowBe4.com