FOCAL POINT
SOLUTIONS GROUP
The Power of Services™

UCG Technologies
A Focal Point Solutions Group Company

Strategic
A Focal Point Solutions Group Company

KnowBe4
Human error. Conquered.

Find Out What Percentage Of Your Employees Is Phish-prone™

Traditional once-a-year Security Awareness Training doesn't hack it anymore. Today, employees are frequently exposed to sophisticated phishing attacks, and your users are now the weak link in your network security. They need to be trained by an expert, and after the training stay on their toes, keeping security top of mind.

The bad guys are bypassing your antivirus end-point security. They are going directly after your end-users, social engineer them to click on a malicious link, compromise the workstation and hack into your network and servers. Next, they steal valuable customer databases, intellectual property, or you become the victim of a cyberheist where they take over your online banking accounts and transfer your organization's money overseas. This is happening as we speak. Thousands of U.S. organizations now are the victim of a cyberheist. The need for Security Awareness Training has become urgent.

The Bad Guys Are Going After Your End-users

Organized, focused and financially motivated hackers try to make end-users click on something and keep their intrusions hidden. There are 100,000 new malware variants released each day, and millions of spear phishing emails are sent each day with those levels continuing to rise. Traditional antivirus products were not designed for these emerging threats. The efficacy of all antivirus suites against fresh phishing attacks which use social engineering and/or zero-day exploits is severely lacking.

> ***"Social Engineering is information security's weakest link."***
> ***– Kevin Mitnick. 'The World's Most Wanted Hacker', IT security consultant.***

Where We Are

Today, cyberheists are costing millions, and 79% of Small and Medium Enterprises (SMEs) have no formal policy or security awareness training program in place. International organized cybercrime is thriving. It is an industry literally raking in billions of dollars. The human side of cyber security is neglected. There is still no national strategy against cyberattacks on private organizations, so small and medium enterprise and non-profits are on their own.

Where We're Going

Now and in the future, an essential element of your defense-in-depth is Security Awareness Training for all employees. And unlike traditional once-a-year sexual harassment training, KnowBe4 allows you to schedule regular Phishing Security Tests to keep employees on their toes so they will not get 'phished', or 'social engineered' and keep security top of mind.

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.

Think Before You Click

KnowBe4 is an IT security company, so our infrastructure was built from the ground up to have a secure, and fault-tolerant cloud-based infrastructure. KnowBe4 was PCI compliant from day one:

- Our Development Group consists of software engineers that have 10+ years of experience in creating secure application.
- Our servers are hardened Linux machines, any critical connections all use secure sockets layer.
- The databases are backed up daily.
- We do not store passwords in plain-text, we use a one-way salted, peppered and 10x encrypyted hash mechanism, in which passwords cannot be retrieved even if we want to.
- Essentially, the data we store consists only of email addresses, and what this address has clicked on. No other data gets stored, and KnowBe4 has done everything to be secure, scalable and reliable.
- As the phishing tests only use standard email/web protocols, and do not include any actual malware, KnowBe4 phishing tests will not introduce any vulnerabilities into your systems.

This Is Where Kevin Mitnick Security Awareness Training™ Comes In

Our Kevin Mitnick Security Awareness Training™ provides you with next-generation on-demand, cloud-based training for employees of any size organization. Why is this product next-gen? First of all, it is the only product that benefits from Kevin's 30-plus years of first-hand hacking experience. Traditional Security Awareness Training is static and gets updated once a year at best. KnowBe4 helps you to keep your employees on their toes with regular simulated phishing attacks. We track the initial tests, next the training itself, and then the after-training tests. You will get detailed before-and-after reports that show the results of the training, and who the culprits are. You will also see the whole organization's Phish-prone graph on your KnowBe4 cloud-based management console.

Where KnowBe4 Is Different From The Others

More and more, you see training companies promote their security awareness training products as 'modular' as if that is something good. They break their training in small modules, split up by security topic, and say that this is better. They say that this is the way people learn and work. It's not. They say that one lesson a month, each with a different security awareness topic, is the best approach. Unless you have an extremely secure environment, it's actually an invitation to a data breach. Would you install a firewall and slowly, over time, block the ports you need to defend? There is a massive problem with this approach.

Security Training Fragmentation Causes A Knowledge Gap

You want all your employees, as soon as possible, to understand and be armed against all attack vectors. Employees should get all the important online dangers in one training session, integrated and reinforced multiple times within in that initial training session. That is the only responsible way to deploy security awareness training. With all employees knowing all the online dangers, there is group agreement and peer pressure in the direction of secure behavior. You don't want to start with training them about phishing and only weeks or months later train them about social networking. That leaves a social engineering hole big enough to drive a truck through. If you want to keep all employees on their toes with security top of mind, do that with continued testing. Sending a simulated phishing attack once a week is extremely effective to keep employees alert, and a proven way to dramatically decrease their Phish-prone percentage.