

# Make Your Employees the Frontline of Cyber Defense.

Let us provide you a full picture of your company's security posture and potential risk, so the employees who were the weakest link in your defense can become its strongest point of protection.



## Cyber-Attacks Are on the Rise

## Solution: Monitor, Train and Phish!



**92.4%**  
of malware is  
delivered via email

Because employees are the core of any business, they will be the main target for cyber criminals. Making sure your people stay up-to-date with cyber security knowledge, and teaching them to recognize threats, is imperative to the security of your business. The threat landscape is constantly evolving, and so should your approach to defense.

### Why You Need an Integrated, Ongoing Program

- ▶ Cyber-attacks are on the rise; particularly among small- and mid-sized businesses.
- ▶ You may have the most up-to-date and strongest security systems in place, but this will be a wasted investment if you don't also train and test your staff.
- ▶ Threats are ever-evolving and become more sophisticated and harder to detect. Regular training on the latest criminal tactics will help mitigate risk.
- ▶ Domain monitoring allows you to be alerted if your credentials are found on the Dark Web

Trained and aware employees are critical to securing an organization, and an effective, ongoing internal security awareness program can help reduce your company's vulnerability, turning the "weakest link" in your cyber defenses into its greatest strength.

### Email Phishing Simulations

Email phishing has become very sophisticated and almost undetectable, as criminals have found ways to make their emails as realistic as possible. Email phishing simulations test employees on how they would respond to a real-life phishing attack. We can send these mock attacks at staggered times, avoiding the "prairie dog effect" where employees warn one another of the email, for the best measurement of all employees' awareness. We'll track which employees have clicked on a phishing email, who has given away their password and who has ignored the email.

### Security Awareness Training

Our Online platform contains easy-to-understand, short and visually engaging training videos include an Online quiz to verify the employee's retention of the training content. As the threat landscape changes, our platform is continuously updated with the most up-to-date relevant training content to keep your line of defense alert and strong.

### Dark Web Monitoring

Cybercriminals traffic and buy stolen credentials so they can infiltrate your networks to steal your data. By monitoring the Dark Web for threat intelligence about stolen user data associated with your company's domains, you can be alerted when a compromise is detected, so that you can respond to stop a potential costly and widespread data breach.



**90%** of security breaches are inadvertent, unintentional, and caused by human error

# Cybersecurity Essentials

Email Phishing Simulations, Security Awareness Training and Dark Web Monitoring



These **Cybersecurity Essentials** offerings are sold as a bundle or à la carte.

## Email Phishing Campaigns

We can send scheduled email phishing campaigns, including customized messages to fit each group or department, at random times during a specified period. With an ever-changing threat, it is important that your employees are exposed to all the latest phishing traps set by criminals.

### Email Phishing Campaigns Include:

- ▶ One Campaign per Month
- ▶ One Campaign Report per Quarter
- ▶ One Report Review per Quarter

## Security Awareness Training

It is not always disgruntled workers and corporate spies who are a threat. Often, it is the non-malicious, uninformed employee. Our easy-to-understand, short and visually engaging training videos end with an online quiz to verify the employee's retention of the training content.

### Security Awareness Training Includes:

- ▶ One Training per Month
- ▶ One Training Report per Quarter
- ▶ One Report Review per Quarter

## Dark Web Monitoring

Employees often use the same password for multiple services on the web, such as CRM, e-commerce sites, and social media. Proactive monitoring for stolen and compromised employee data on the dark web allows us to detect when a problem arises, before a major breach occurs.

### Dark Web Monitoring Includes:

- ▶ 24/7 Dark Web Monitoring
- ▶ Responses to Alerts, as Necessary
- ▶ One Report per Month

Your employees are your first and primary line of defense against online crime. Equip them with the knowledge and skills they need to protect themselves—and your business—from criminal elements.

 Taking Care of Business. That's IT.

centrexIT.com | 619.651.8700 | 12232 Thatcher Court, Poway, CA 92064