IntegraMSP
PARTNERSHIPS BUILT ON INTEGRITY

SECURITY AWARENESS
CHAMPION'S GUIDE

CHEAT CODES FOR BEATING CYBERCRIME
WITH SECURITY AWARENESS TRAINING

IT'S NOT SAFE TO GO ALONE, TAKE THIS:

THE EFFECTIVENESS OF SECURITY AWARENESS TRAINING

Security awareness training isn't an exciting solution to cybersecurity problems. It doesn't thrill you with innovation or wow you with next-level technology. But do you know what it does do? It works.

This powerful, affordable secret weapon empowers your business to defeat cybercrime - and we've got the stats to prove it.

- Regular security awareness training reduces cybersecurity incidents by 70%
- 62% of businesses do not do enough cybersecurity awareness or phishing resistance training
- The number one cause of a data breach or cybersecurity disaster is human error
- 86% of CISOs in a recent survey listed improving security standards as a top priority
- 45% of workers receive no security awareness training at all
- 78% of employees are aware of the risks of suspicious links in emails but will click them anyway
- 93% of security professionals agree that strong human and machine security protection is the most effective way to prevent disaster
- Even the "least effective" programs have a seven-fold ROI
- Most cybersecurity awareness training programs have a 37-fold ROI
- 49% of workers doubt their ability to identify a social engineering attack

GAME OVER:
THE PRICE OF FAILURE

No one wants to endure an expensive, messy, and disruptive cybersecurity disaster. Unfortunately, current trends indicate that the chance of a company being targeted by a cyberattack is growing quickly, and the cost of being caught flatfooted has never been higher.

- 80% of businesses have experienced an increase in cybercrime
- Cybercrime damage is expected to reach $6 trillion by 2021
- 30% of companies will experience at least 1 data breach each year
- Data breaches have increased worldwide by 50%
- GDPR violations have cost companies more than $126 million in penalties

CYBERCRIME LEADERBOARDS: 2020 VS. 2019

Phishing has increased by **667%**

Cloud-based attacks are up more than **625%**

Business email compromise fraud is up **200%**

Ransomware attacks have grown by **148%**

Credential stuffing attacks have surged **41%**

EXPERT

TIPS & TRICKS

UPDATE TRAINING REGULARLY

Studies show that workers only retain the knowledge that they've gained about things like phishing for about 4 months.

TRAIN EVERYONE, EVERY TIME

74% of data breaches involve access to a privileged account like an executive or administrator

STAY ALERT TO DARK WEB DANGER

It may sound like a nebulous threat, but more than 60% of the information on the Dark Web can harm businesses.

GET SERIOUS ABOUT PASSWORD HYGIENE

More than 60% of all cybercrime is committed with stolen, cracked, or compromised passwords.

REMOTE WORKERS NEED EXTRA TRAINING

43% of remote workers admit to making mistakes that resulted in cybersecurity repercussions for their companies.

CREDENTIAL STUFFING

TYPE OF THREAT:
Brute Force Attack

TARGETS:
Email and systems access gateways

DANGER:
Medium

CHALLENGE RATING:
Difficult

This increasingly common attack type is a dangerous foe. Fueled by the massive amounts of data available in Dark Web markets and data dumps, cybercriminals throw as many passwords as they can at entry points in a blizzard of blows, hoping that one will be a key to the door. Credential Stuffing is a risk that only grows with time, as more stolen information like password lists and user records makes its way to the Dark Web.

DEFEAT IT

A few simple precautions can help companies get the last laugh against Credential Stuffing:

MULTIFACTOR AUTHENTICATION

Requiring a second code for access to systems and data means that even if cybercriminals do happen to acquire a password that works, they'll need a second code to get in, neutralizing the threat.

DARK WEB MONITORING

Keep an eye on credential security by having business credentials monitored 24/7/365 for compromise. If one turns up in a Dark Web market, you're notified fast to stop password-based attacks before they start.

ACHIEVEMENT UNLOCKED!

Super Speedy Defender
A new cyberattack
is launched every 39 seconds.

BUSINESS EMAIL COMPROMISE

TYPE OF THREAT:
Phishing

TARGETS:
Staffers, prefers highly privileged accounts

DANGER:
Medium

CHALLENGE RATING:
Difficult

Take phishing, blend it with disguises, and add the patience to play a long con, and you've created a Business Email Compromise attack. Cybercriminals turn to this format for two purposes: to steal money from a business directly, or to use a company's trustworthy reputation to steal money from other businesses through impersonation.

DEFEAT IT

IMPROVE EVERYONE'S PHISHING DEFENSE

Make sure that everyone on a company's network is up-to-speed on common phishing threats and how to handle them, especially highly privileged users and executives – with phishing simulation campaigns and online security awareness training.

CONTROL ACCESS FROM SINGLE SIGN-ON LAUNCHPADS

Instead of setting individual permissions per application, give each user on a network their own unique launchpad. Not only does it eliminate pain points for tech staff, it also allows access to be quickly removed from a compromised account.

ACHIEVEMENT UNLOCKED!

Cybercriminal Unmasked

Business Email Compromise cost companies about $1.7 billion last year.

PASSWORD COMPROMISE

TYPE OF THREAT:
Hacking & Theft

TARGETS:
All employees, with special emphasis on administrators

DANGER:
Medium

CHALLENGE RATING:
Difficult

Password sharing, recycling, and mishandling is an ancient and terrible cybersecurity foe that just keeps reappearing. Through everything from writing down passwords, creating weak passwords, and sharing passwords among staffers, password compromise is always a disaster.

DEFEAT IT

SECURE IDENTITY AND ACCESS MANAGEMENT

A password alone isn't a good enough way to keep systems and data safe no matter how you make it. A multifunctional secure identity and access management solution lets businesses use multiple shields to guard their access points in one cost-effective move.

WATCH FOR SNEAK ATTACKS

A staffer could be recycling or reusing an already compromised password – especially if it's one they use for both work and home applications. Add a guardian that runs up the red flag if a protected password hits the Dark Web.

ACHIEVEMENT UNLOCKED!

Hold the Door

80% of data breaches last year were caused by password compromise.

RANSOMWARE

TYPE OF THREAT:
Phishing & Malware

TARGETS:
Any organization in any industry

DANGER:
High

CHALLENGE RATING:
Very Difficult

The monster under the bed for cybersecurity professionals is ransomware. This nasty parasite grabs ahold of a business through phishing to install malware that steals data and locks up systems. Dangerously easy to catch, incredibly difficult to dislodge, and extremely expensive to recover from, ransomware can be so damaging that it puts companies out of business.

DEFEAT IT

STAY ON TOP OF IT

Ransomware is most often delivered through email. Frequent, easy-to-understand phishing resistance training that includes engaging videos and online testing makes every user more wary about email threats.

HIDE THE KEYS TO THE KINGDOM

You know what makes a cybercriminal's job even easier? The administrator passwords to your servers, databases or applications. Secure Shared Password Vaults add an extra layer of security between intruders and highly privileged passwords while still enabling IT staffers to find exactly what they need when they need it in a central repository.

ACHIEVEMENT UNLOCKED!

Evading Capture
Two in five businesses have fallen prey to ransomware.

INSIDER THREATS

TYPE OF THREAT:
Varied

TARGETS:
Business systems and data

DANGER:
High

CHALLENGE RATING:
Very Difficult

The number one cause of cybersecurity disasters is human beings. Insider threats don't only include malicious actors like employees selling their login credentials or stealing information. They also include negligent, careless, rushed, tired, and ignorant employees making cybersecurity blunders like forgetting to lock a database or falling for a phishing email, making insider threats a two-headed monster for businesses.

DEFEAT IT

MAINTAIN HIGH SECURITY STANDARDS

The combined power of multifactor authentication, single sign-on, easy remote management, and individual user LaunchPads gives IT teams the tools that they need to mitigate most staffer hijinks.

GUARD THE BACK DOOR

One of the most devastating and heartbreaking threats to businesses is the possibility that a rogue employee is selling their data or systems access on the Dark Web, so keep watch 24/7/365 using human and machine intelligence to spot danger before it comes knocking on the door.

ACHIEVEMENT UNLOCKED!

Super Sentinel

Insider threats haven't just climbed by 47%, they've also grown 31% more expensive, making stopping them crucial for business success.

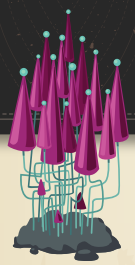
PHISHING

TYPE OF THREAT:
Social Engineering

TARGETS:
Any user through email, text, social media, messaging, calls, fraud, and deception.

DANGER:
Epic

CHALLENGE RATING:
Extreme



Phishing is the poisoned swamp that spawns many of today's most dangerous cyberthreats, like its nastiest child, Ransomware. It's also the number one threat that businesses face today, and it's very slippery. Phishing can arrive in a plethora of disguises like:

SPEAR PHISHING

A carefully crafted, highly convincing email that fraudulently directs the victim to "update account credentials", handing them over to cybercriminals.

SMISHING

An innocent looking text from a "coworker" (who is actually a cybercriminal) asking for an administrator password to complete a routine, annoying task.

VISHING

A voicemail that contains a request for access from a "contractor" (who is really a bad actor) who just needs a password for your database to complete a maintenance task.

DEFEAT IT

The best way to avoid falling victim to a phishing attack is to refuse to take the bait. Use the perfect combination of the latest threat information presented in bite-sized pieces, simple remote campaign management and deployment, and regularly updated lessons in eight languages to transform employees from the biggest security threat into the biggest security asset for a business.

MULTIFUNCTIONAL DEFENSE

Put more than one layer of defense between the bad guys and the heart of any business with the multipurpose, dynamic protection that's included as a standard feature of this innovative, award-winning secure identity and access management solution.

ACHIEVEMENT UNLOCKED!

Bulletproof

90% of all incidents that end in a data breach start with a phishing email.

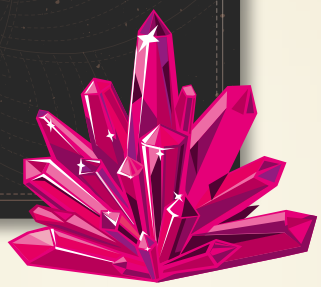
LEVEL UP!

PRESTIGE CLASS UNLOCKED:

SECURITY AWARENESS CHAMPION

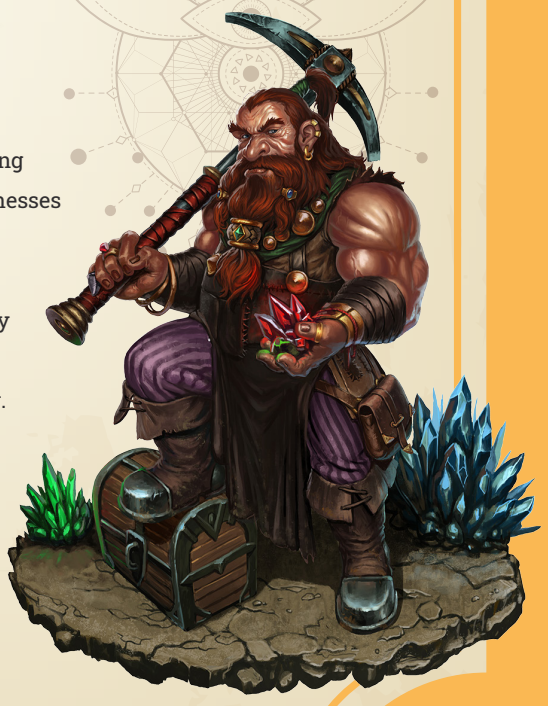
REWARDS & LOOT

Dark Web activity has increased by more than 300% in the last year



The cybersecurity landscape is fraught with peril, and that won't be changing anytime soon. Investing in security awareness and phishing resistance training doesn't just pay off now, it also keeps paying dividends over time to keep businesses (and budgets) safe.

95% of cybersecurity professionals expect a dramatic increase in cybersecurity risk from new cybercrime technology and IoT devices in the next two years. Phishing resistance training makes staffers 84% less likely to fall for phishing. 93% of security professionals agree that strong human and machine security protection is the most effective way to prevent disaster.



DON'T PUT OFF STRENGTHENING CYBER RESILIENCE WITH THIS SECRET WEAPON.

UNBEATABLE WINNING STRATEGY

Even in challenging economic conditions, cybersecurity isn't a game where any business can afford to lose points by making budget cuts that weaken your defenses. Defeat the biggest business cybersecurity threats with this unbeatable winning strategy.

MAKE THIS KILLER COMBO MOVE TO KEEP SYSTEMS AND DATA SAFE TODAY AND TOMORROW:

- Dynamic security awareness training that makes employees strong defenders
- Engaging phishing resistance training that includes up-to-date threats
- Secure identity and access management that keeps access points safe
- Real-time Dark Web threat intelligence 24/7/265 to alert you to danger fast

START YOUR ORGANIZATION'S TRANSFORMATION FROM VULNERABLE TO PROTECTED NOW, BECAUSE YOUR THREAT METER IS RISING.

IntegraMSP
PARTNERSHIPS BUILT ON INTEGRITY

SECURITY AWARENESS
CHAMPION'S GUIDE

CHEAT CODES FOR BEATING CYBERCRIME
WITH SECURITY AWARENESS TRAINING

www.IntegraMSP.com | sales@integramsp.com

11232020