Inside Today's Biggest Cybercrime Risk & How to Fight Back

#MSP

APR. 2021

$3.89 US

THE PHISH FILES

IntegraMSP

PARTNERSHIPS BUILT ON INTEGRITY

NO ONE WANTS TO BECOME A STATISTIC

Learn the truth about cybercrime in today's world - get the facts about phishing and phishing-related cybercrime to see just how dangerous this menace has become.

- More than 60% of cybercriminals use phishing as their primary form of attack
- 65% of organizations have experienced a phishing attack in the last year
- Over 80% of all cyberattacks are phishing based
- Phishing attacks have shot up by 667% since the start of the COVID-19 pandemic
- A new phishing attack is launched every 39 seconds
- 90% of incidents that end in a data breach start with a phishing email

TUMULTUOUS WORLD EVENTS

Overall cybercrime has been steadily increasing each year, but phishing risk has increased exponentially in the last 12 months. Tumultuous world events, economic challenges, technological advancement, and Dark Web growth have all come together to create ideal conditions for phishing-related cybercrime to thrive – and cybercriminals have been quick to capitalize on that opportunity.

- The damage related to cybercrime is projected to hit $6 trillion annually by 2021
- Ransom payment demands increased by more than 30% in the last 12 months
- In a year-over-year comparison, downtime costs from cyberattacks have climbed by 75%
- The average duration of business interruption from a cyberattack has increased by around 50%
- The amount of revenue generated by cybercrime on the Dark Web jumped by 65% this year

WHY PHISHING IS CHEAP AND EFFECTIVE

More than 60% of cybercriminals use phishing as their primary form of attack. Why? Phishing is cheap and effective. Not only is it the perfect weapon to use against businesses in general, it's especially effective against companies that are supporting a remote workforce and relying on email as their primary form of communication.

- Even novice cybercriminals can conduct phishing campaigns (including software and hosting) for as little as $30 per month
- The amount of data available to bad actors on the Dark Web has grown by more than 300% in 2 years
- More than 60% of the data available on the Dark Web can do harm to businesses
- 43% of remote workers have made cybersecurity errors that endangered their company
- An estimated 55% of remote workers rely on email as their primary form of communication

PHISHING IS TODAY'S BIGGEST CYBERSECURITY THREAT

Phishing is today's biggest cybersecurity threat. Just one attack can devastate a company – and the chance of a business experiencing a phishing attack has never been higher.

- Ransomware attacks have skyrocketed by 148%
- 74% of phishing attacks involve credential compromise or password theft
- 67% of data breaches in the last year were caused by social engineering attacks
- Business email compromise fraud has grown by 20%
- Spear phishing has boomed with a surge of more than 600%

PHISHING INCLUDES:

There are many variations on phishing, and that can make it hard to spot and stop.

- Credential Theft
- Social Engineering
- Spear Phishing & Whaling
- Business Email Compromise (BEC)
- Ransomware & Malware
- Smishing & Vishing

CYBERCRIMINALS USE THE STOLEN CREDENTIALS

THE SCAM

A phishing attack that's designed to capture someone's password or other credentials.

THE GOAL

To acquire credentials that allow cybercriminals to log into company systems and applications. Highly privileged passwords that belong to administrators or executives are especially prized.

THE SETUP

› Credential theft can happen through email, SMS text, instant messaging – even by phone. This slippery foe can wear many disguises like:

- › A message that directs the recipient to enter a password on a webpage
- › An alert that it's time to update your password
- › An inquiry about a password that's needed for a seemingly routine task
- › A notice that an app has changed, and you'll need to create a new account

THE DAMAGE

Cybercriminals use the stolen credentials to walk right in the front door of a company, enabling them to install malware, steal data, or gain access to systems without raising suspicion until it's too late.

PHISHING ATTACKS DESIGNED TO FOOL PEOPLE

THE SCAM

A phishing attack that's designed to drive the recipient to take an action.

THE GOAL

To capture passwords, obtain access to systems and data, steal information or trick the recipient into downloading malware.

THE SETUP

- All phishing attacks contain an element of social engineering, because they're all designed to fool people into taking the bait. Some common techniques used in social engineering include:
  - Impersonating a contractor or colleague to obtain sensitive information
  - Convincing someone to provide information or credentials in a way that violates policy
  - Using fake pressures like a deadline or emergency to gain access to information or systems
  - Fooling someone into filling out a form that captures information
  - Tricking the recipient into downloading a malware-laden document
  - Promising a reward or faking a contest to encourage recipients to provide information

THE DAMAGE

Cybercriminals lure unsuspecting staffers into doing their dirty work for them by unleashing ransomware and malware or giving them access to valuable data without raising suspicion.

PHISHING ATTACK FEATURING PERSONALIZED DETAILS TO LURE YOU IN

THE SCAM

A phishing attack featuring personalized details in the lure that add believability to increase the likelihood that the recipient will take the bait.

THE GOAL

To lure incautious recipients into taking an action that compromises their credentials, obtains sensitive information, or deploys malware including ransomware.

THE SETUP

- Cybercriminals use personalized information about the targets to craft emails that seem legitimate, often powered by information obtained from Dark Web markets and data dumps. These lures can include:
  - "Whaling" messages directed at executives or other highly privileged targets
  - Email from the recipient's bank, credit card company, or a similar source
  - Free downloads from organizations that the recipient belongs to
  - Requests for donations from charities that are in the recipient's sphere
  - Fake political email from candidates or parties
  - Attachments like brochures or notices from trusted sources like a government agency
  - Spoofed messages from the recipient's regular service providers, suppliers, or other vendors

THE DAMAGE

Spear phishing is growing increasingly more dangerous as the amount of data available to cybercriminals allows them to create better bait. It's commonly used to capture credentials, steal information, cause a data breach, or deploy malware and ransomware.

THE FAKE EMAIL ATTACK

THE SCAM

A phishing attack that uses fake email to request payment from a business

THE GOAL

Getting businesses to transfer money or provide sensitive financial information under false pretenses

THE SETUP

› The tricky part of spotting BEC attacks is that they're carefully crafted to be so believable that they fly right under the radar. They're primarily targeted to ensnare people within an organization who handle matters of payment or can access funds quickly, like:

- › Administrative assistants who routinely process payments for small expenses
- › Executives who can order bills to be paid without oversight
- › Clerks who make vendor payments
- › Budget controllers that pay for recurring services
- › Accounting personnel who regularly renew licenses or pay government fees

THE DAMAGE

BEC enables cybercriminals to get paid directly and capture financial information like banking information and executive credit card numbers to facilitate fraud and other financial damage.

TO INFECT COMPUTERS WITH MALICIOUS SOFTWARE

THE SCAM

A phishing attack that packs a punch by delivering nasty software surprise

THE GOAL

To infect computers with malicious software that enables cybercrime or to encrypt systems and data, making them inaccessible without a “key” obtained from the cybercriminals that did the deed.

THE SETUP

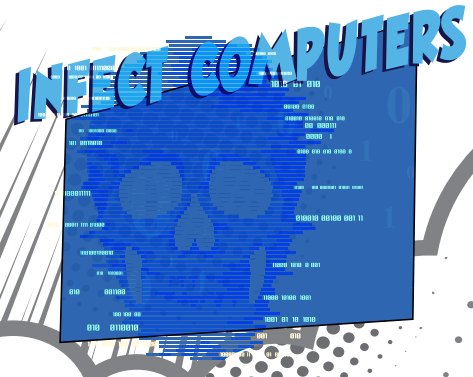
› Malware and ransomware are weapons that can be wielded by cybercriminals against business, infrastructure, private, and public sector targets.

Some common ways that malware and ransomware are used include:

- › Taking control of manufacturing, production or industrial equipment
- › Secretly copying data to a server controlled by cybercriminals
- › Installing payment skimmers to steal credit card numbers or divert online payment funds
- › Encrypting systems and data to disable operations and demanding a payment for the key
- › Snatching up important data like medical research, schematics, records, formulas, or databases
- › Stealing sensitive data and threatening to release it on the Dark Web without a ransom payment
- › Shutting down internet enabled systems from transportation systems to IoT devices
- › Enabling hacking and intrusion by nation-state actors

THE DAMAGE

Malware and ransomware are the most dangerous results of phishing and can be used to destroy infrastructure, harm research and development efforts, shut down production lines, drive a business into bankruptcy, facilitate espionage and terrorism, or even as a weapon of war.



DON'T FALL FOR THE BAIT

THE SCAM

Instead of an email, targets receive phishing messages through SMS text, instant messaging or even old-fashioned phone calls.

THE GOAL

To obtain passwords, credentials, sensitive information or financial data.

HOW IT HAPPENS

› These reasonable requests don't seem dangerous because they're carefully crafted to appear routine. Most phishing training focuses on email, making staff less cautious about messages and calls, and increasing opportunity for cybercriminals thanks to social media and today's instant messaging heavy office culture.

A typical smishing or vishing attack might start with:

- › A text message from a supplier reminding the target of an overdue payment
- › A Teams message from a colleague asking for an urgently needed password
- › A call from a service provider asking the target to start using a new payment system
- › A voicemail asking for an invoice payment by phone to be called in to a certain phone number
- › An instant message from a contractor who needs a credential giving them access to a database

THE DAMAGE

Unprepared staffers who fall for this bait can easily give bad actors the keys to the kingdom, enabling them to install malware or ransomware, steal data, or cause other harm while flying under the radar.

FIGHT BACK WITH A POWERFUL TOOL

BullPhish ID is the ideal phishing resistance training solution for any business. It's packed with features that make it perfect for both in-office and remote training – and a powerful tool that raises overall cybersecurity awareness in an organization without breaking the bank.

- Enables any business to conduct regular (and successful) security awareness training
- The user-friendly interface makes it easy to use, with no special tech knowledge required
- Easy management allows for custom employee grouping and automated campaign deployment
- Online testing measures absorption to show who needs more training

SECURITY AWARENESS AND PHISHING RESISTANCE TRAINING

It's no mystery why security awareness and phishing resistance training with BullPhish ID is a smart move. The innovative tools, consistent updates, thoughtfully designed content, and customer support that businesses get with BullPhish ID provides great value and gets the job done right.

- Over 80 plug-and-play phishing simulation kits are available, with 4 new kits each month
- Preloaded kits come complete with every component needed -- no extras or add-ons needed
- More than 50 engaging, animated training videos are available in 8 languages
- New training content is added frequently, including COVID-19 threats
- Custom scheduling enables trainers to vary campaign dates and times as needed

RAPIDLY GROWING CYBERCRIME

Rapidly growing cybercrime risks aren't slowing down – especially now that more businesses are supporting a remote workforce. BullPhish ID can empower any business to mitigate phishing threats by transforming their employees from their biggest cybersecurity risk into their biggest cybersecurity asset.

- 60% of businesses lose unrecoverable data as a result of a phishing attack
- An organization will be hit by a ransomware attack every 14 seconds in 2020
- 50% of companies that fail to block a phishing attack are infected with ransomware or malware
- 73% of organizations view strong cybersecurity as a major contributor to business success
- Security awareness training can reduce the impact of a cyberattack by more than 70%

Increased cybersecurity awareness and phishing resistance is a business essential that provides great short-term and long-term ROI – because it pays to keep staffers ready to face the latest cybersecurity threats like phishing when one fatal click could cost a business everything.

CYBERCRIME RISKS AREN'T

SLOWING DOWN!

www.IntegraMSP.com | sales@IntegraMSP.com