
Monsters
of
Cybersecurity
ID AGENT
A Kaseya COMPANY

Tales From the Breach

The world of digital risk can be a scary place. Horrors lurk around every corner, just waiting for the opportunity to pounce on an unsuspecting business and deploy malware, steal data and unleash other terrible attacks. That thing under the bed? It's ransomware. The scratching at the window? That's spear phishing. And the eyes that are upon you from the closet? That's a data breach. The monsters of cybersecurity are a very real danger for every business and are every IT professional's nightmare.

But there is hope that businesses can fend off these foul fiends and stay safe from trouble. Read on to learn how to protect organizations against the ghouls and ghosts that are headed their way and prevent future curses. Taking sensible precautions against cybersecurity beasts that go bump in the night is the smart way to ensure that every business has the tools they need to become monster slayers instead of monster chow.

13 Frightening Facts About Cybercrime

```
make_float4(-1.0f, +1.0f, +1.0f, 1.0f),
make_float4(+1.0f, +1.0f, +1.0f, 1.0f),

make_float4(-1.0f, -1.0f, -1.0f, 1.0f),
make_float4(-1.0f, -1.0f, +1.0f, 1.0f),
```

A HUMAN ELEMENT IS INVOLVED IN 85% OF BREACHES.

THE NUMBER OF BREACHES THAT USED RANSOMWARE DOUBLED IN 2020.

ABOUT 61% OF BREACHES INVOLVED MISUSE OF CREDENTIALS.

PHISHING REMAINS THE TOP THREAT ACTION THAT RESULTED IN A BREACH.

- The FBI recorded a 69% increase in reported cybercrime in 2020.
- About 61% of organizations worldwide experienced a damaging ransomware incident in 2020.
- IT teams are facing a 64% year-over-year increase in ransomware threat volume.
- About 60% of companies that suffer a cyberattack like ransomware go out of business within a year.
- In a cybercrime survey, 42% of respondents said that their organization had been compromised because of a bad, stolen, reused or cracked password in 2020.
- Around 80% of IT professionals in a recent survey said that their organizations have faced an increase in the number of phishing attacks that they're combatting in 2021.
- More than 80% of reported security incidents are phishing-related.
- A whopping 74% of organizations in the United States have fallen victim to a successful phishing attack.
- About 34% of data breaches in 2020 involved internal actors.

CYBERATTACK FACT VS. FICTION

MYTH 1

SECURITY AWARENESS TRAINING DOESN'T WORK, IT'S WASTED MONEY.

That's not true. Security awareness training works and is a highly effective way to reduce an organization's chance of experiencing a cybercrime disaster. It reduces the risk of a data breach by up to 70% and reduces the cost of phishing by more than 50%.

cx = CENTERX * w;
cy = CENTERY * h;

MYTH 2

AN EMAIL FROM A BIG COMPANY LIKE MICROSOFT IS ALWAYS SAFE.

Nope. Spoofing and brand impersonation are popular cyberattack tactics because people believe that emails from major companies are safe. However, this is a dangerous misconception. In fact, Microsoft is the most widely impersonated brand, making up 45% of 2020's brand impersonation frauds. Email spoofing and brand impersonation continue to be growing risks that every business needs to be alert to — spoofing ballooned by more than 220% in 2020.

cx = CENTERX * w;
cy = CENTERY * h;

MYTH 3

IT'S OK TO KEEP USING AN OLD PASSWORD AND USE THE SAME PASSWORDS AT WORK AND AT HOME.

No, it's never okay. Huge lists of passwords stolen in previous cyberattacks around the world are available on the dark web for cybercriminals to use in attacks. An estimated 60% of passwords that appeared in one or more breaches in 2020 were recycled or reused. Businesses are in even greater danger if an employee reuses a password at work that they've used at home. At least 60% of people reuse their favorite passwords across multiple sites regularly, driving up the chance that it's already compromised.

cx = CENTERX * w;
cy = CENTERY * h;

MYTH 4

A CYBERATTACK WILL ONLY COME FROM OUTSIDE THE COMPANY.

Unfortunately, no. No one wants to think that one of their teammates might have dark motives, but malicious insiders caused about 25% of data breaches in 2020. That damage can also be hard for companies to detect, giving bad actors more time to wreak havoc. An insider incident takes more than twice the amount of time to detect than other intrusions, which can lead to ransomware or a data breach.

MYTH 5

WE'RE TOO SMALL FOR FANCY THINGS LIKE MULTIFACTOR AUTHENTICATION.

Absolutely not. Just under 45% of all cyberattacks are aimed at small to medium-sized businesses every year. Every business of every size is at risk of a cybersecurity mishap, whether it comes from a phishing email, a cyberattack or a bad password. In fact, 70% of SMBs had employee passwords compromised in the past year. A small security upgrade like multifactor authentication stops almost all password-related cyberattacks. It's also a compliance requirement in many industries.

FACT

Cybersecurity is part OF EVERYONE'S JOB.

CORRECT.

Businesses must emphasize that every employee is part of the security team in order to build a strong security culture and avoid trouble in today's volatile risk landscape. No employee should fear losing their job for reporting a mistake or security problem, and security awareness training should never be used as a punishment. Unfortunately, less than half of security professionals feel that they have the support they need from leadership to do that, while 10% feel they have no support at all.

ROGUES GALLERY: ARE YOU READY to Face MONSTERS OF CYBERSECURITY?

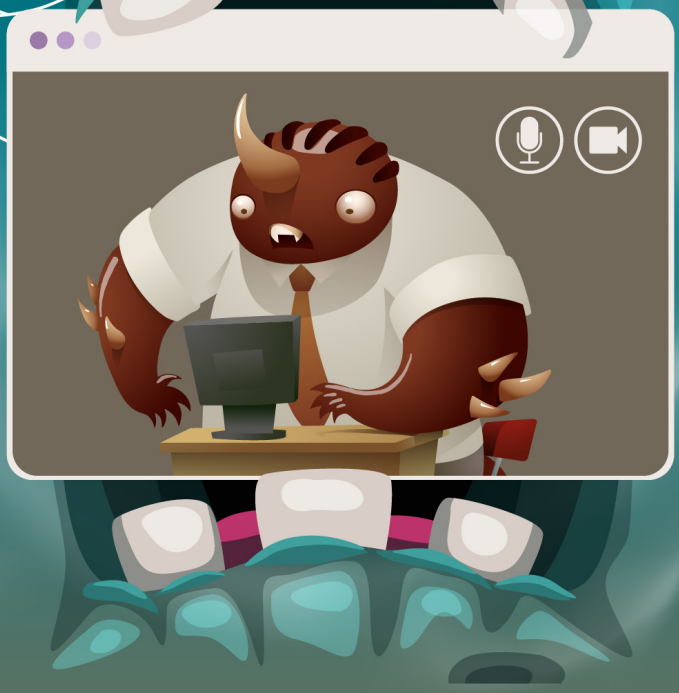
TWO IN FIVE SMALL AND MEDIUM-SIZED BUSINESSES FACED A FEARSOME MONSTER LIKE RANSOMWARE IN AN EXPENSIVE, DAMAGING CYBERSECURITY INCIDENT IN 2020 — AND MOST OF THEM WEREN'T READY FOR THE FIGHT.

Waiting until the boogeyman arrives at your doorstep may be a fast track to disaster, but taking sensible precautions against trouble can give you a chance to save your data and your sanity.

- About 50% of SMBs have no plan in place to handle a cybersecurity incident or cyberattack.
- Just over 20% of companies have adopted formal, enterprise-wide security response plans.
- Almost 50% of companies have conducted no training for employees regarding security awareness.
- Only 14% of small businesses rate their ability to mitigate cyber risks and attacks as highly effective.
- An estimated 25% of SMB owners stated that they had to spend $10,000 or more to resolve one cyberattack.

Preparation is the magic bullet that helps businesses defeat the cybercrime horrors that lurk around every corner. By taking sensible steps to bolster security, you increase company cyber resilience, which lets everyone sleep a little easier at night.

RANSOMWARE



What really scares IT professionals? The monster under the bed: ransomware. This devastating behemoth is a killer and it's becoming more common. In the past six months alone, ransomware attacks shot up 150% compared to all of 2020. Let's dispel the shadowy mystery of ransomware with smart strategies to keep systems and data safe.

HOW IT ATTACKS

Ransomware is most likely to reach businesses as the nasty cargo of a phishing email. It can also be unleashed into systems through the direct action of bad actors.

THE DAMAGE IT CAN CAUSE

Data Theft: Cybercriminals will demand a ransom for the return or decryption of the victim's data.

However, that doesn't mean the victim will get it back unharmed. Less than 8% of businesses can recover all their data after a ransomware incident even if they pay the ransom. The criminals that steal your data will make money if you don't pay too — personal and financial data is a hot seller in the booming dark web data markets.

System Lockdown: Ransomware can also bring any business to a grinding halt by rendering everything from office systems to factories to pipelines inoperable. Companies impacted by ransomware lost an average of six working days to system encryption. An estimated 37% of those companies experienced downtime that lasted one week or more.

WARD OFF THIS MONSTER

Ransomware is a terrifying prospect for any company to face, but don't let it paralyze you with fear. Taking these precautions can help you defend against ransomware:

Security Awareness Training

Protecting businesses from ransomware starts by protecting them from phishing. Around 90% of ransomware arrives at businesses as the poisonous cargo of a phishing email. Making sure that every employee knows what to look for to spot and stop these pernicious threats will keep them from being tricked by bad actors into making a ghastly mistake.

Secure Identity and Access Management

Making sure that only the right people have access to sensitive systems, databases or financial information goes a long way towards preventing hackers or malicious insiders from using their illicit access to unleash ransomware – 10% of ransomware attacks are carried out by bad actors directly. Keep the ghosts out of your machines by regulating access to avoid trouble.

PHISHING

As a cyberattack that can change form and function quickly, phishing is a tricky foe. Like a magic portal, phishing is the gateway for a host of other terrors. Phishing attacks can be used to conjure up horrors like business email compromise, malware or CEO fraud. It is almost always a disaster if a business falls prey to a phishing attack – an estimated 80% of all cybersecurity incidents involve phishing.

HOW IT ATTACKS

Phishing messages attempt to use social engineering to entice victims to click a dangerous link, open an attachment rife with malware or give up their password through trickery.

THE DAMAGE IT CAN CAUSE

Facilitating a Cyberattack: A phishing email is the vehicle of choice for cybercriminals, allowing them the freedom and flexibility to do their dirty business by deploying malware or stealing credentials that can move them along to the next phase of their attack, like encrypting data in a ransomware incident.

Data Breaches: Part of the allure of phishing is its versatility and ease of use, enabling new cybercriminals and seasoned veterans alike to quickly sneak into a company's environment and snatch their valuable data – 90% of incidents that end in a data breach start with a phishing email.

WARD OFF THIS MONSTER

At first glance, phishing may seem like the smallest monster you'll face but don't let it fool you — it packs the biggest bite. Taking these precautions can help you defend against phishing:

Phishing Resistance Training

When everyone is on the lookout for phishing emails, the company's chances of falling prey to phishing drastically reduce. An emphasis on phishing resistance as part of a consistent security awareness training program can reduce the number of staffers likely to click on a phishing email by half in just six months.

Multifactor Authentication

Cybercriminals are always looking to phish a password from an employee to use for other dastardly deeds — the more privileged the better. Take the power away from a phished password with multifactor authentication, a magical guardian that stops up to 99% of password-based cybercrime.

Malicious Insider

Is everyone in the company really on the same team? Insider threats include non-malicious acts, like a careless employee error, and malicious acts like an employee stealing data. Even a low-level malicious insider has the potential to do devastating damage. This shapeshifting fiend is especially dangerous because it could be anyone — almost 25% of insider threats are due to malicious insiders.

HOW IT ATTACKS

Malicious insiders act deliberately to benefit themselves at the expense of the organization. They might do things like steal proprietary information, deploy malware, steal privileged credentials or even sell their own password as part of the thriving cybercrime-as-a-service economy on the dark web.

THE DAMAGE IT CAN CAUSE

Lost Money & Growth: Malicious insider threats have surged, increasing by 47% in two years. The cost of these incidents has grown commensurately, jumping 31% to $11.45 million in 2020.

Loss of Corporate Secrets: 71% of malicious insider incidents are done for financial gain, and that includes stealing client lists, customer records, formulas, blueprints and other sensitive information.

WARD OFF THIS MONSTER

No one wants to face the specter of a traitor on their team, but sadly, it happens to businesses every day. Taking these precautions can help you defend against malicious insiders:

Watch the Dark Web

If employees are going to sell access, data or other valuable information, they'll sell it on the dark web. Dark Web ID enables companies to keep an eye on credential compromises from the inside as well by alerting companies as soon as a protected credential is spotted.

Trust No One

Everyone needs to be on the lookout for suspicious activity, like employees using thumb drives unexpectedly, accessing systems and data that they shouldn't be able to get to, or attempting to get around security. Zero-trust security also helps prevent malicious insider activity by using tools like secure identity and access management to make sure the right people can access the right things at the right levels, and only after providing proof that they are who they say they are.

Business Email Compromise

This horror lurks in the shadows, striking quickly and stealthily to inflict tremendous damage on an organization. The Federal Bureau of Investigation Internet Crimes Complaint Center (FBI IC3) declared business email compromise (BEC) the most expensive cyberattack of 2020, even beating headline-makers like ransomware. Business email compromise rose by 14% overall in 2020 and by up to 80% in some sectors, making it a foe that must be vanquished quickly.

HOW IT ATTACKS

This villain specializes in fraud and has many tricks up its sleeve, like utilizing legitimate (or freshly stolen) email accounts from a trusted business to fraudulently acquire money, personal information, credit card numbers and other data, or falsifying service provider invoices requesting wire transfers.

THE DAMAGE IT CAN CAUSE

Financial Ruin: BEC will ruin a company's finances faster than any other cyberattack. In fact, business email compromise is responsible for 64 times as many losses as ransomware.

In 2020, BEC costs increased rapidly, from $54,000 in the first quarter of 2020 to $80,183 in the second quarter as cybercriminals took advantage of the opportunity presented by a newly remote workforce and chaotic world events.

WARD OFF THIS MONSTER

Business email compromise is an insidious menace to every business that can drive organizations to financial ruin. Taking these precautions can help you defend against BEC:

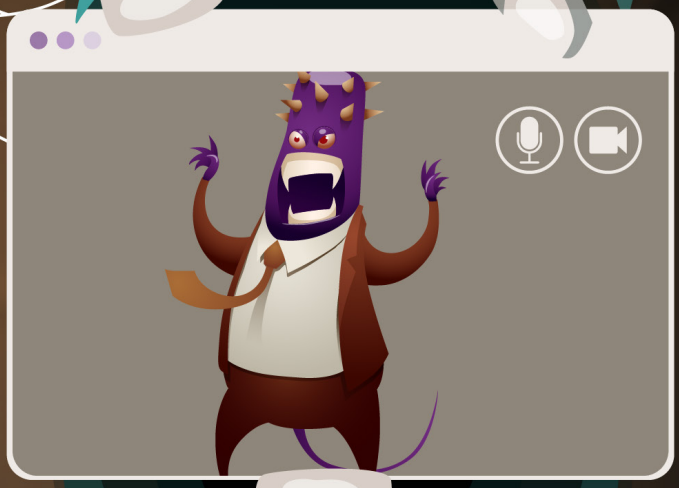
Improve Cyber Resilience

Increasing an organization's cyber resilience will help it survive crippling blows like BEC. Making remote operations easy for tech staffers and using automated security tools quickly increases cyber resilience to help businesses keep moving forward in adverse conditions.

Build a Strong Security Culture

Creating a strong security culture is important to keeping businesses safe from phishing-based threats like BEC. Educating employees to help them spot trouble is crucial. Security awareness training can reduce an organization's chances of a damaging cybersecurity incident like this by up to 70%.

CREDENTIAL COMPROMISE



Credential compromise is the monster you never expect, popping up to wreak havoc at any time, without warning. Obtaining one employee password can give cybercriminals a clear path to the heart of a business, enabling them to perpetrate other nasty attacks like deploying ransomware. Credentials were the most frequent type of information stolen in data breaches worldwide in 2020.

HOW IT ATTACKS

The biggest vector for credential compromise is recycled employee passwords — 60% of passwords that appeared in more than one breach in 2020 were reused. Phishing is another prime vector for credential compromise as cybercriminals use sophisticated, socially engineered attacks to trick employees out of their passwords.

THE DAMAGE IT CAN CAUSE

Wreaking Havoc: Easy, unrestricted access to an organization is a cybercriminal's dream. Credential compromise is just the opening gambit in many other cyberattacks – and the more privileged the credential is, the more damage cybercriminals can do with it.

Over 40% of IT professionals said that their organization had been damaged by a cybersecurity incident like a data breach because of a bad, recycled or stolen password in 2020.

WARD OFF THIS MONSTER

Credential compromise is a horror that can haunt businesses again and again, constantly trying to slip past your defenses. Taking these precautions can help you defend against credential compromise:

Dark Web Monitoring

Don't wait until it's too late to find out that an employee credential has been compromised. Use dark web monitoring to make sure company credentials aren't hanging out in dark web data markets or dumps and get notified 24/7/365 if one pops up.

Single Sign-On

Create a single launchpad for every employee that takes them to every application they use with one login. Not only is it convenient, but single sign-on enables tech staffers to quickly isolate and remove permissions for a compromised credential, limiting the scope of potential damage.

Next Generation

THE NEXT GENERATION OF MONSTERS

Nothing stays the same forever no matter how eternal it may seem. As technology changes and tumultuous events rock the world, the cybersecurity threats that businesses face evolve too, growing and mutating into a new breed of monsters for IT teams to fight.

Nation-State Threat Actors

Recent attacks on infrastructure targets as well as government and business strikes have highlighted the danger that an increasingly connected world faces from cybercriminals with nationalist motivations. This category will continue to grow, especially around malware like ransomware — the most commonly used tool of nation-state cybercriminals.

Brand Impersonation

Businesses are doing more online than ever before, creating a veritable flood of business email, especially corporately branded email from companies like Microsoft, which is the top brand impersonation target. Cybercriminals aren't wasting any time cashing in on the new opportunities this flood produces, especially spoofing. As much as 80% of all spear phishing includes brand impersonation.

Next-Generation Ransomware and Its Variants

One of the fastest growing areas of cybercrime is ransomware. As security evolves to defeat their current schemes, ransomware practitioners have to keep innovating to keep up. In order to keep their revenue high, bad actors never stop working to create new ransomware variants that enable them to stay a step ahead of the security curve. Today's fashionable ransomware variant is double extortion — a nasty curse that encrypts systems and steals data in one attack to net twice the profit. This variant accounted for 50% of ransomware attacks in 2020, and there are always new varieties on the horizon.

Monster-Hunting Tips

AFTER LOOKING AT THIS ROGUES GALLERY, IT'S CLEAR HOW NASTY SOME OF THESE MONSTERS CAN BE. FOLLOWING THE TIPS MENTIONED ABOVE CAN HELP YOU WARD OFF DANGER AND INCREASE CYBER RESILIENCE TO KEEP SYSTEMS AND DATA SAFE.

HERE ARE SOME OTHER SECURITY ACTIONS YOU CAN TAKE TO BOOST YOUR CYBER RESILIENCE:

- Review your entire security buildout with an expert to make sure you're not missing anything. Even the smallest crack in your defense is big enough for cybercrime to slip through.
- Prioritize building a strong cybersecurity culture. When everyone feels like they are part of the security team, everyone will be more inclined to do their part to spot and stop threats like phishing.
- Establish a strong password policy that discourages reuse and recycling of passwords and encourages using a password manager instead of sticky notes.
- Communicate clearly that no one will be fired for reporting a potential security incident immediately, and that it is okay to ask for help about security topics without being penalized.
- Never use security awareness training as a punishment for employees who make security mistakes, or single out people in meetings or emails who have made errors.
- Emphasize to employees that they should never, ever share their passwords with anyone else (even someone in the company) or store their passwords unsafely.
- Employ security automation whenever possible to lower incident response times and reduce alert fatigue for the security team while lowering security and incident costs.
- Make sure that everyone from the interns to the C-suite knows how to handle email safely and how to inform the correct people if they have a question or problem.
- Require everyone at every level to complete regular cybersecurity awareness training — no exceptions. Although phishing targets everyone, attacks like BEC are more likely to happen to executives.
- Create and test incident response plans for cyberattacks to improve incident response time, reduce cost and make sure that everyone is on the same page if the worst happens.

Horrors Lurk Around Every Corner - Be Prepared for Trouble

Security awareness training will reduce an organization's chances of falling victim to a cyberattack while also building a strong security culture that keeps risk in check. As long as you're consistent about training every employee at every level, security awareness training wards off many monsters.

Don't be haphazard – a Usenix study showed that security awareness training is forgotten over time. Test subjects were trained once with retention tested four, six, eight, ten and twelve months later, and the results were unequivocal – the longer they went without training, the worse they performed.

Security awareness training has a great ROI. Companies under 1,000 employees can see an ROI of 69% from a training program and an estimated ROI of 562% for organizations with more than 1,000 employees.

A U.K. study showed that at the beginning of training, 40% to 60% of employees are likely to open malicious links or attachments. However, consistent cybersecurity awareness training made a huge difference in employee behavior. In follow-up testing, after about six months of training, the percentage of employees who took the bait dropped by 20% to 25%. Further training produced a steeper drop. After three to six months of more training, the percentage of employees that opened phishing messages dropped to only 10% to 18%.

BullPhish ID makes it easy to run comprehensive, effective security awareness training for organizations of any size. Our training is perfect for employees with any level of tech knowledge and features security best practices in bite-sized pieces with no "geek speak."

BullPhish ID makes it easy to teach employees to spot and stop the threats they face every day with a wide variety of training options, including premade plug-and-play phishing kits or fully customized the content to reflect your industry's unique threats.

Employees won't just learn about phishing – they'll brush up on password handling, ransomware, compliance and other security topics as well. Lessons including memorable videos and online testing are available in eight languages and new modules are added every month.

Best of all, with BullPhish ID, the training process is smooth for everyone. Deliver training through a personalized user portal that makes it a snap for employees to take the right courses at the right time. Plus, our intuitive admin portal enables administrators to easily create training campaigns, track progress and report on each employee's success.

WHAT'S THAT SCRATCHING AT THE GATE?

Keep the Doors and Windows Locked

Secure identity and access management helps ensure that you only let the right ones in. A foundational element of zero-trust security maintaining tight access control makes it harder for the bad guys to slip in unnoticed to strike your organization even if they have help inside.

Passly is the multitool solution you need to make secure identity and access management easy and affordable. Get multiple, key security components in one solution at a rate far below the competition, especially when compared to the total cost of products from multiple vendors. Passly also ensures that a zero-trust framework is within reach to set every organization up for compliance success in the future. These features make it the perfect choice for companies of any size.

Multifactor authentication

This is a requirement for most industries' compliance standards and CISA compliance standards. According to Microsoft, it is 99% effective in preventing password-based cybercrime such as using a stolen (or purchased) password and hacking.

Single sign-on

Make sure that access controls stay tight by ensuring the right people have access to the right things at the correct levels. SSO gives tech staffers an edge when responding to security incidents that can prevent major damage by making it simple for them to isolate a compromised access point.

Passly also gives you quick and easy access to SSO applications and passwords, with the ability to automatically fill in those credentials for web logins. You'll also enjoy automated password resets, secure shared password vaults, seamless integration with over 1,000 business applications and robust remote management capabilities that reduce tech staff stress and decrease incident response times.

DON'T LET A CYBERATTACK SNEAK

Up on You - Keep an Eye on Potential Threats

The dark web is home to a dangerous shadow economy perpetuated by villains. It might also be home to your company's stolen credentials. Watching out for unexpected nasty surprises coming from the dark web is a smart idea.

Dark Web ID is the ideal solution to act as a dark web lookout for every company, giving executives and IT teams peace of mind, knowing that there's an expert on the job who will alert them to stolen credentials before the bad guys have a chance to notice and use them. Protect your business from unpleasant credential compromise surprises with 24/7/365 dark web monitoring that puts human and machine intelligence to work for you.

Are your company's credentials already compromised? You may be in danger right now and not even know about it.
Find every one of your company's compromised credentials in minutes with dark web search, enabling you to fix those security gaps immediately.
The dark web may be shrouded in mystery but Dark Web ID gives you a clear picture of your real-time dark web risk with simple reports and automated alerts. Plus, it's easy to quickly get protection in place by leveraging out of-the-box integrations with popular PSA platforms to create a frictionless alerting and mitigation process, so you never miss a security event.

GET POWERFUL PROTECTION

FROM THE

MONSTERS OF CYBERSECURITY

IT'S TIME TO DEFEND YOUR ORGANIZATION AGAINST THE DANGERS BROUGHT TO YOUR DOORS EVERY DAY IN THIS DARK, SCARY CYBERSECURITY LANDSCAPE. AND YOU DON'T HAVE TO GO THROUGH IT ALONE. WE CAN HELP.

VISIT OUR WEBSITE FOR MORE INFORMATION

CONTACT A SECURITY EXPERT FOR A ONE-ON-ONE DEMO

BULLPHISH ID, PASSLY & DARK WEB ID - DEMO VIDEOS