



# The OnPar Report

## “Technology Tips to Transform Your Business”

### We've Partnered with ID Agent to Monitor the Dark Web For Your Compromised Business Credentials!

**28,500.** That's the average number of data records per company, including credentials, that are compromised during a data breach. Our Dark Web ID Credential Monitoring detects compromised credentials in real-time on the Dark Web and notifies you immediately when these critical assets are compromised, before they can be used for identity theft, data breaches, or other crime.

Digital credentials such as usernames and passwords connect you and your employees to critical business applications, as well as online services. Unfortunately, criminals know this — and that's why digital credentials are among the most valuable assets found on the Dark Web.

Far too often, companies that have had their credentials compromised and sold on the Dark Web don't know it until they have been informed by law enforcement — but by then, it's too late. According to National Institute of Standards and Technology (NIST), small and medium-sized businesses may have more to lose than larger organizations, because cybersecurity events can be costly and threaten their survival.



**Cybersecurity doesn't have to be complicated. The first step to protecting your business is understanding your risk. Get your free dark web scan and make sure your business hasn't been compromised:**

<https://www.onpartech.com/dark-web/>

#### Free Dark Web Scan

Dark Web ID reports 80,000+ compromised emails daily, with 24/7/365 monitoring.

#### What We Monitor

- Hidden Chatrooms
- Private websites
- Peer-to-peer networks
- IRC (Internet relay chat) channels
- Social media platforms
- Black market sites
- 640,00 botnets

#### What Your Business Receives

- Security awareness
- Password managers
- Multifactor authentication
- Constant Monitoring
- Data Leak Prevention
- Vulnerability and patch management
- Peace of Mind

Dark Web ID is the industry's only commercial solution available to detect customers' compromised credentials in real-time on the Dark Web. It vigilantly searches the most secretive corners of the Internet to find compromised data associated with your customers' employees, contractors and other personnel.

[Click to learn more about OnPar's remedy package today](#)

## Have You Heard of Microsoft 365?

Take advantage of our free Microsoft 365 Webinar to learn more about this integrated solution designed to help businesses achieve more together anywhere it matters, with always-on security.

If the following applies, consider attending our free webinar:

- Are you looking to reduce the overall cost of managing your IT?
- Are you interested in moving your business to the cloud and reducing or eliminating on-premise servers?
- Are you in need of a solution that allows your employees to communicate on-the-go?
- Do you want to protect your company data with always-on security?
- Are you looking to safeguard your customer data, company data, and intellectual property?
- Do you want to simplify the setup and management of employee's devices?



Plus the 8th person to register and attend this webinar will win a brand new Xbox One S Starter Pack!

Register Now At: <http://www.onpartech.com/puzzle>



This Xbox Could Be Yours!

## Get Started Today With Microsoft Azure

With Microsoft Azure, you can capitalize on consistent, self-service application access management so your organization gains agility and flexibility while reducing your IT costs. You can also gain remote access to on-premise applications.

### 5 Strategies for Moving Your Business To The Cloud:

1. Move as high up the technology stack as possible: Cloud providers offer solutions at numerous levels. User higher-level cloud offerings when you can.
2. It's not all-or-nothing, so prioritize your projects: Your business doesn't have to make large-scale shifts to a public cloud provider all at once. Build experiences as you go by identifying lower-risk, high-reward areas for initial deployments.
3. IT best practices are more important than ever: IT professionals use cloud services as an opportunity to focus on higher-value technology projects allowing you to focus on your business.
4. Extend your data center: Cloud service providers can provide ways to extend your on-premise infrastructure with cloud-based offerings.
5. Take the opportunity to do some housekeeping: Over time, most organization amass "technical debt" - the side effect of taking shortcuts and making rush decisions. Moving to the cloud is a great opportunity to consolidate and realign services.

[Click To Get Started!](#)

## Our Featured Case Study: Component Estimator



Component Estimator is a material takeoff company that has been in business for over 5 years. Mike King, president of Component Estimator, is responsible for managing a team of 10 employees and overseeing sales, operations, and accounting. Component Estimator provides services that support lumber yards and builders throughout the country. Such services include the ability to breakdown building blueprints and outline the material needed to construct those buildings.

Component Estimator was using multiple platforms to manage their daily internal communication operations which included GoDaddy, Drop box, Go-To-Meeting, and various Office Suites. In addition, they were also utilizing two meeting platforms: the free skype application and Go-To-Meeting. Go-To-Meeting limited their meeting capabilities based on how many licenses were rented, while the free version of Skype required purchasing credits for outgoing calls

With Component Estimator growing in size, it was apparent that the company and its employees needed to invest in a higher level of organization. **Keep reading...**

---

### Monthly Tech Tip: Rebound from Embarrassing Email Mistakes in a Flash in Outlook

At some point, we've all hit Send, only to realize one-quarter of a second later that it was sent to the wrong person, sent without the attachment, or sent with errors. Our favorite Office 365 tip and trick is the ability to get that email back before it's seen by the recipient. Save yourself embarrassment in 2018 by recalling an email before it arrives. With message recall, a message that you sent is retrieved from the mailboxes of the recipients who haven't yet opened it. You can also substitute a replacement message. For example, if you forgot to include an attachment, you can try to retract the message, and then send a replacement message that has the attachment.

With message recall, a message that you sent is retrieved from the mailbox of the recipients who haven't yet opened it. You can also substitute a replacement message. For example, if you forgot to include an attachment, you can try to retract the message, and then send a replacement message that has the attachment.

Message recall is available after you click Send and is available only if the recipient has an Exchange account within the same organization.



**[Click To Learn How To Enable This Feature For Your Outlook!](#)**

# 39%

## Percentage of adults in the U.S. using the same or very similar passwords for multiple online services, which increases to 47% for adults age 18-29

Passwords are a twentieth-century solution to a twenty-first century problem. Unfortunately, user names and passwords - the most common digital credentials used today - are all that stands between your employees and vital online services including corporate networks, social media sites, e-commerce sites and others. A good security practice is to use a completely different password for every service, but the fact is that nearly 40% of Americans replicate the same or very similar passwords for each service they use.

Pew Research Center, "Americans and Cybersecurity", January 2017

### How Are Credentials Compromised?



#### Phishing

- Send e-mails disguised as legitimate messages
- Trick users into disclosing credentials
- Deliver malware that captures credentials



#### Malvertising

- Inject malware into legitimate online advertising networks
- Deliver malware to visitors that captures credentials



#### Watering Holes

- Target a popular site: social media, corporate intranet
- Inject malware into the code of the legitimate website
- Deliver malware to visitors that captures credentials



#### Web Attacks

- Scan Internet-facing company assets for vulnerabilities
- Exploit discovered vulnerabilities to establish a foothold
- Move laterally through the network to discover credentials



Federal Financial Institutions Examination Council (FFIEC), "Joint Statement: Cyber Attacks Compromising Credentials", March 2015

### What Can an Attacker Do with Compromised Credentials?



Send Spam from Compromised Email Accounts

Deface Web Properties and Host Malicious Content

Install Malware on Compromised Systems

Compromise Other Accounts Using the Same Credentials

Exfiltrate Sensitive Data (Data Breach)

Identity Theft

Please Seriously Consider Taking Advantage of Our Free Dark Web Scan. Don't Put Your Business and Employees at Risk. [Click To Sign Up](#)