Cyber Score Report

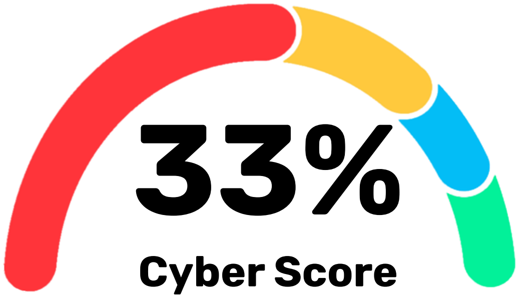
CASTILE
SECURITY

ACME Dental
am1st.com

Critical vulnerabilities in outdated software pose the most significant threat to your business security.

Key Takeaway

55
Dark Web
Breaches

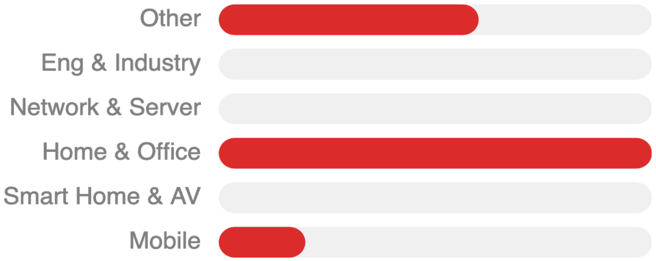


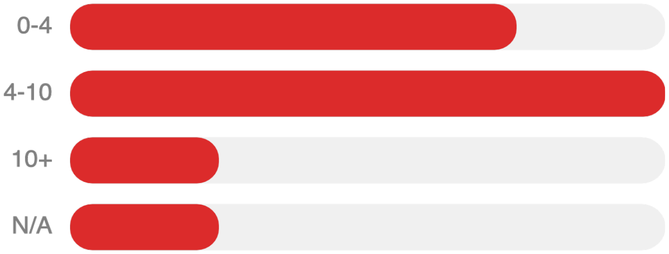
RISK OVERVIEW

Cyber threats are a reality, swift and silent. Your business is your single largest investment. Regular cyber audits act as your early warning system, pinpointing risks before they strike. It's about being proactive, not reactive. Strengthen your defenses, ensure your business's resilience and prosperity in the face of digital dangers.

134 Exploitable software vulnerabilities found

5 Aging assets more than 4 years old





ACTION PLAN

This is your 3 Step Cyber Action Plan to reduce security risks:

Cyber Score Report

DARK WEB REPORT SUMMARY

Why it matters:

Discovering your employees' work emails and passwords on the dark web spells serious trouble. It's a gold mine for cybercriminals. Armed with your team's emails and passwords from the Dark Web, they can raid your assets in seconds, not days. This isn't just risky; it's a direct threat to your business's survival.

55 Email accounts for sale on the Dark Web

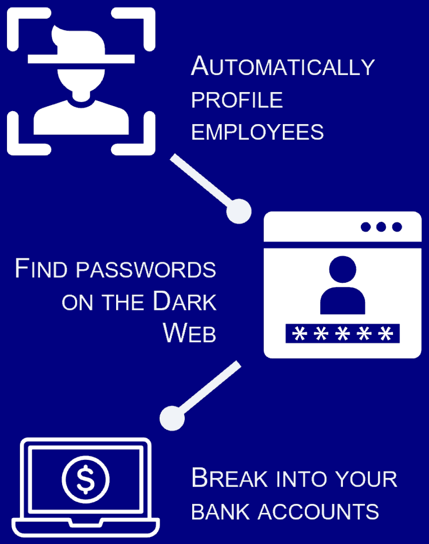
10 Total Accounts Scanned

Top Accounts	Name	Position	Breaches
bdunaway@am1st.com			15
eball@am1st.com	Eric Ball	Managing Director	14
dguthrie@am1st.com	David Guthrie	Vice President	12
kwiese@am1st.com	Katerina Wiese	Vice President	8
mholloway@am1st.com	Matt Holloway		6
abyrne@am1st.com	Amy Byrne	Client Care Officer	0
privacy@am1st.com			0
e@am1st.com			0
rocky@am1st.com			0
dholloway@am1st.com			0

How to fix it:

By implementing Multi-Factor Authentication and ongoing Dark Web monitoring, even if passwords are exposed, your business remains sealed. Turn your vulnerabilities into strengths, safeguarding your future and setting you apart from the competition.

3 STEP ATTACK



AUTOMATICALLY PROFILE EMPLOYEES

FIND PASSWORDS ON THE DARK WEB

BREAK INTO YOUR BANK ACCOUNTS

What could go wrong:

Using off-the-shelf marketing tools, criminals find your employees' details, then match them with credentials from the Dark Web. Armed with emails & passwords, they effortlessly access banking, email, and cloud services. This simple but effective method exposes your business to serious financial risks and data breaches.

Cyber Score Report

CASTILE
SECURITY

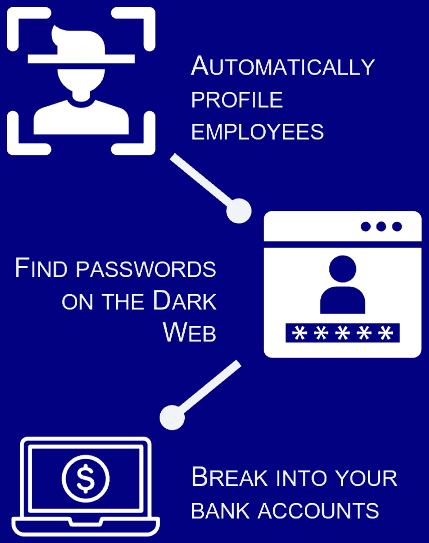
Dark Web Full Report

Most Recent Breaches

55 Email accounts for sale on the Dark Web **10** Total accounts scanned

Breach Date	Email Address	Breached Account
2024-06-22	bdunaway@am1st.com	Zacks (2024)
2024-02-28	bdunaway@am1st.com	DemandScience by Pure Incubation
2024-02-28	dguthrie@am1st.com	DemandScience by Pure Incubation
2024-02-28	eball@am1st.com	DemandScience by Pure Incubation
2024-02-28	kwiese@am1st.com	DemandScience by Pure Incubation
2024-02-28	mholloway@am1st.com	DemandScience by Pure Incubation
2021-04-08	dguthrie@am1st.com	LinkedIn Scraped Data (2021)
2021-04-08	eball@am1st.com	LinkedIn Scraped Data (2021)
2020-11-04	bdunaway@am1st.com	Cit0day
2020-11-04	dguthrie@am1st.com	Cit0day
2020-11-04	eball@am1st.com	Cit0day
2020-11-04	kwiese@am1st.com	Cit0day
2020-11-04	mholloway@am1st.com	Cit0day
2020-10-03	bdunaway@am1st.com	Gravatar
2020-10-03	dguthrie@am1st.com	Gravatar
2020-10-03	eball@am1st.com	Gravatar
2020-10-03	kwiese@am1st.com	Gravatar
2020-10-03	mholloway@am1st.com	Gravatar
2020-09-28	bdunaway@am1st.com	Nitro
2020-05-10	bdunaway@am1st.com	Zacks

3 STEP ATTACK



AUTOMATICALLY PROFILE EMPLOYEES

FIND PASSWORDS ON THE DARK WEB

BREAK INTO YOUR BANK ACCOUNTS

What could go wrong:

Using off-the-shelf marketing tools, criminals find your employees' details, then match them with credentials from the Dark Web. Armed with emails & passwords, they effortlessly access banking, email, and cloud services. This simple but effective method exposes your business to serious financial risks and data breaches.

Cyber Score Report

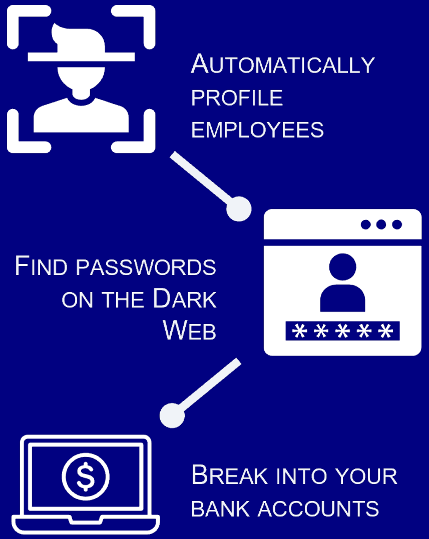
Dark Web Full Report

1/1 - All Monitored Accounts

55 Email accounts for sale on the Dark Web **10** Total accounts scanned

Top Accounts	Name	Position	Breaches
bdunaway@am1st.com			15
eball@am1st.com	Eric Ball	Managing Director	14
dguthrie@am1st.com	David Guthrie	Vice President	12
kwiese@am1st.com	Katerina Wiese	Vice President	8
mholloway@am1st.com	Matt Holloway		6
abyrne@am1st.com	Amy Byrne	Client Care Officer	0
privacy@am1st.com			0
e@am1st.com			0
rocky@am1st.com			0
dholloway@am1st.com			0

3 STEP ATTACK


Automatically profile employees
Find passwords on the Dark Web
Break into your bank accounts

What could go wrong:

Using off-the-shelf marketing tools, criminals find your employees' details, then match them with credentials from the Dark Web. Armed with emails & passwords, they effortlessly access banking, email, and cloud services. This simple but effective method exposes your business to serious financial risks and data breaches.

Cyber Score Report

EMAIL IMPERSONATION REPORT

Why it matters:

Email fraud can devastate a small business where criminals can forge your identity to trick clients or employees, risking finances, and reputation. Without SPF, DKIM, and DMARC, your email domain is an open door to such impersonation and deceit.

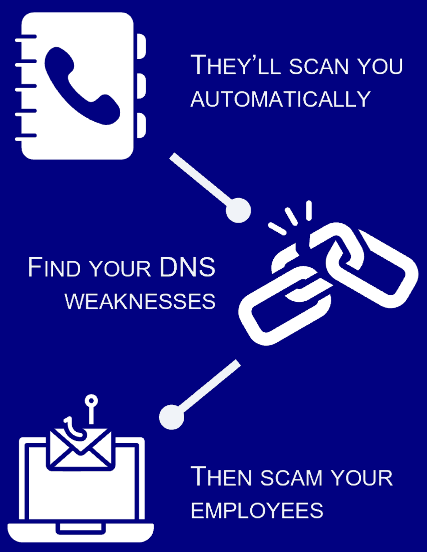
Status	Record
Pass	v=spf1 include:spf.protection.outlook.com include:spf.smarsh.com -all
Fail	No DKIM records found.
Fail	No DMARC records found. We recommend you use: v=DMARC1; p=reject;
Pass	Microsoft Exchange Online Protection gateway detected

How to fix it:

Implementing SPF, DKIM, and DMARC seals your email domain against imposters, safeguarding your business's communications. This trio verifies emails' authenticity, blocking fraudsters, protecting your finances, and maintaining your reputation. It's a clear step towards securing your business's integrity and trustworthiness.

CASTILE SECURITY

3 STEP ATTACK



THEY'LL SCAN YOU AUTOMATICALLY

FIND YOUR DNS WEAKNESSES

THEN SCAM YOUR EMPLOYEES

What could go wrong:

DNS records are the internet's phone book. Criminals can easily spot your email system's weaknesses, as straightforward as reading the phone book. They can then automatically send emails to your employees, masquerading as you, the CEO, or HR. Who wouldn't open an email titled 'Vacation Policy Updates' from HR?

Cyber Score Report

Asset Risk Report

Why it matters:

Outdated software and vulnerable devices are open invitations for cyber thieves, jeopardizing your revenue and customer trust. With weekly vulnerabilities emerging, ignoring updates transforms your business into a prime target for data theft and ransomware attacks.

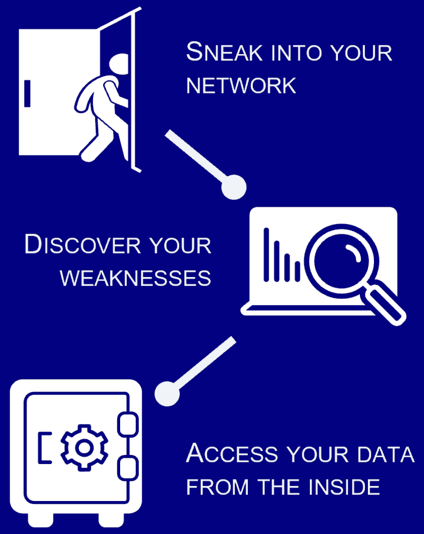
134 Exploitable software vulnerabilities found **9** Total assets scanned

Priority	Vulnerability
Critical	jQuery XSS allows execution of untrusted code via <option> elements
High	Outdated jQuery version can be exploited for security breaches
Medium	Diffie-Hellman Key Exchange triggers server-side DHE calculations, causing DoS
Medium	IP Forwarding Enabled allows unauthorized access to network traffic
Low	jQuery allows execution of text/javascript responses via cross-domain Ajax requests
Low	jQuery XSS allows attackers to construct malicious payloads more easily
Low	jQuery object extensions allow property injection, leading to prototype pollution
Low	jQuery 1.2 XSS allows execution of untrusted code
Low	jQuery load method executes enclosed script logic, enabling cross-site scripting
Low	jQuery XSS exploit allows malicious code injection through text method

How to fix it:

By deploying regular software updates, rigorous network configurations, and advanced protection protocols, you not only close the door on potential attackers but also ensure it stays closed. Proactive maintenance and monitoring services mean that your network remains resilient against the ever-evolving threat landscape.

3 STEP ATTACK



Sneak into your network

Discover your weaknesses

Access your data from the inside

What could go wrong:

Neglected and outdated devices are significant cyber risks. They're ideal for attackers to spread malware. One phishing email can trigger a domino effect paralyzing your whole company. With new software exploits daily, such oversights quickly escalate from minor issues to major security breaches.

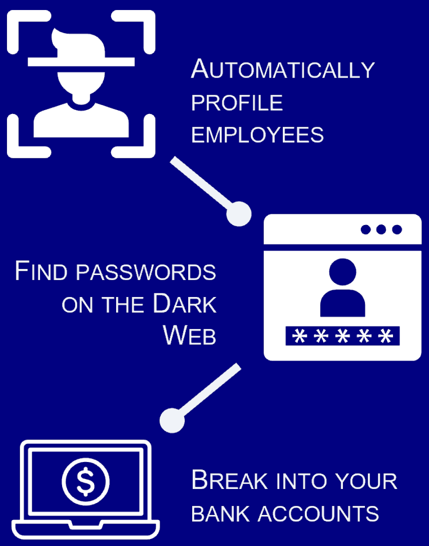
Cyber Score Report

Asset Inventory

1/1 - All Monitored Assets

Risks	IP Address	Vendor	Age	Category
46	192.168.2.1	Sagemcom Broadband SAS	3	
46	192.168.2.1	Sagemcom Broadband SAS	3	
10	192.168.2.11	Micro-star Intl	9	Home & Office
6	192.168.2.14	Ieee Registration Authority	3	Home & Office
6	192.168.2.10	Shanghai Simcom Limited	9	Mobile
6	192.168.2.62	G-pro Computer	16	Home & Office
6	192.168.2.16		0	
5	192.168.2.16	Intel Corporate	5	Home & Office
3	192.168.2.12	GL Technologies (Hong Kong) Limited	5	Home & Office

3 STEP ATTACK



AUTOMATICALLY PROFILE EMPLOYEES

FIND PASSWORDS ON THE DARK WEB

BREAK INTO YOUR BANK ACCOUNTS

What could go wrong:

Using off-the-shelf marketing tools, criminals find your employees' details, then match them with credentials from the Dark Web. Armed with emails & passwords, they effortlessly access banking, email, and cloud services. This simple but effective method exposes your business to serious financial risks and data breaches.

Cyber Score Report

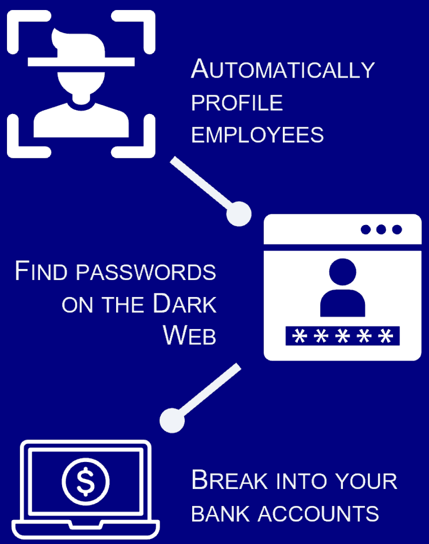
CASTILE SECURITY

Vulnerability Inventory

1/7 - All Monitored Risks

Priority	IP Address	Risk Family	Vulnerability
Critical	192.168.2.1	Web application...	jQuery 1.0.3 < 3.5.0 XSS Vulnerability
Critical	192.168.2.1	Web application...	jQuery 1.0.3 < 3.5.0 XSS Vulnerability
High	192.168.2.1	Web application...	jQuery End of Life (EOL) Detection - Linux
High	192.168.2.1	Web application...	jQuery End of Life (EOL) Detection - Linux
Medium	192.168.2.1	SSL and TLS	Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability...
Medium	192.168.2.1	General	IP Forwarding Enabled - Active Check
Medium	192.168.2.14	General	IP Forwarding Enabled - Active Check
Medium	192.168.2.10	General	IP Forwarding Enabled - Active Check
Medium	192.168.2.62	General	IP Forwarding Enabled - Active Check
Medium	192.168.2.16	General	IP Forwarding Enabled - Active Check
Medium	192.168.2.1	SSL and TLS	Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability...
Medium	192.168.2.1	General	IP Forwarding Enabled - Active Check
Low	192.168.2.1	Service detection	HTTP Server type and version
Low	192.168.2.1	SSL and TLS	SSL/TLS: Certificate - Self-Signed Certificate Detection
Low	192.168.2.1	SSL and TLS	SSL/TLS: Certificate - Subject Common Name Does Not Match...
Low	192.168.2.1	General	ICMP Timestamp Reply Information Disclosure
Low	192.168.2.1	Service detection	Services
Low	192.168.2.1	SSL and TLS	SSL/TLS: Report Non Weak Cipher Suites
Low	192.168.2.1	SSL and TLS	SSL/TLS: Collect and Report Certificate Details
Low	192.168.2.1	Windows	SMB log in

3 STEP ATTACK



Automatically profile employees

Find passwords on the Dark Web

Break into your bank accounts

What could go wrong:

Using off-the-shelf marketing tools, criminals find your employees' details, then match them with credentials from the Dark Web. Armed with emails & passwords, they effortlessly access banking, email, and cloud services. This simple but effective method exposes your business to serious financial risks and data breaches.

Cyber Score Report

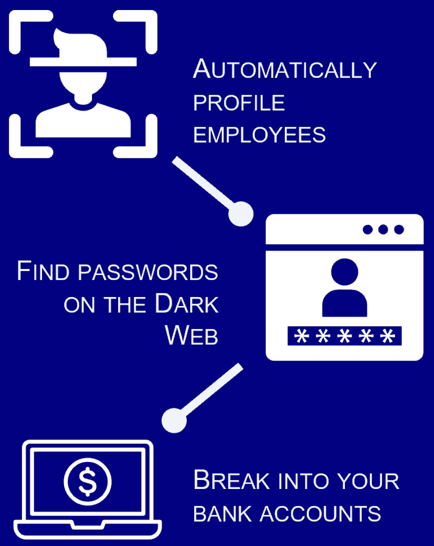
CASTILE SECURITY

Vulnerability Inventory

2/7 - All Monitored Risks

Priority	IP Address	Risk Family	Vulnerability
Low	192.168.2.1	SSL and TLS	SSL/TLS: Certificate Too Long Valid
Low	192.168.2.1	Windows	Check for Accessible Registry (Windows SMB Login)
Low	192.168.2.1	SSL and TLS	SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
Low	192.168.2.1	SSL and TLS	SSL/TLS: Version Detection
Low	192.168.2.1	SSL and TLS	SSL/TLS: HTTP Strict Transport Security (HSTS) Missing
Low	192.168.2.1	Product detection	OS Detection Consolidation and Reporting
Low	192.168.2.1	Service detection	DNS Server Detection (TCP)
Low	192.168.2.1	SSL and TLS	SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
Low	192.168.2.1	SSL and TLS	SSL/TLS: HTTP Public Key Pinning (HPKP) Missing
Low	192.168.2.1	SSL and TLS	SSL/TLS: HPKP / HSTS / Expect-CT Headers sent via plain HTTP
Low	192.168.2.1	Service detection	Unknown OS and Service Banner Reporting
Low	192.168.2.1	Service detection	Hostname Determination Reporting
Low	192.168.2.1	Windows	SMB Login Successful For Authenticated Checks
Low	192.168.2.1	Service detection	HTTP Server Banner Enumeration
Low	192.168.2.1	Service detection	SMB/CIFS Server Detection
Low	192.168.2.1	SSL and TLS	SSL/TLS: Hostname discovery from server certificate
Low	192.168.2.1	Web application…	Web Application Scanning Consolidation / Info Reporting
Low	192.168.2.1	Web application…	HTTP Security Headers Detection
Low	192.168.2.1	SSL and TLS	SSL/TLS: Safe/Secure Renegotiation Support Status
Low	192.168.2.1	SSL and TLS	SSL/TLS: Untrusted Certificate Detection

3 STEP ATTACK



Automatically profile employees

Find passwords on the Dark Web

Break into your bank accounts

What could go wrong:

Using off-the-shelf marketing tools, criminals find your employees' details, then match them with credentials from the Dark Web. Armed with emails & passwords, they effortlessly access banking, email, and cloud services. This simple but effective method exposes your business to serious financial risks and data breaches.

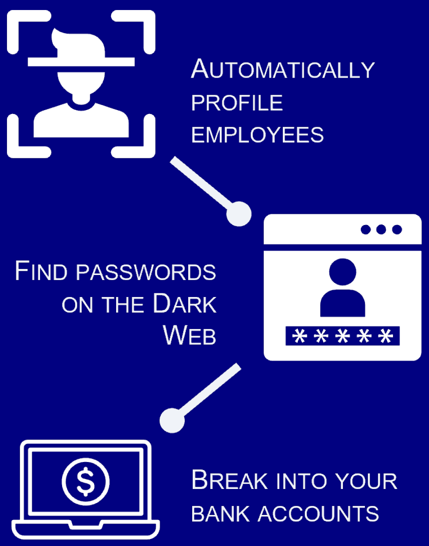
Cyber Score Report

Vulnerability Inventory

3/7 - All Monitored Risks

Priority	IP Address	Risk Family	Vulnerability
Low	192.168.2.1	Service detection	SMBv1 Enabled - Active Check
Low	192.168.2.1	Web application...	jQuery < 3.0.0 XSS Vulnerability
Low	192.168.2.1	Web application...	jQuery < 1.9.0 XSS Vulnerability
Low	192.168.2.1	Web application...	jQuery < 3.4.0 Object Extensions Vulnerability
Low	192.168.2.1	Web application...	jQuery 1.2 < 3.5.0 XSS Vulnerability
Low	192.168.2.1	Web application...	jQuery < 1.9.0 XSS Vulnerability
Low	192.168.2.1	Product detection	jQuery Detection Consolidation
Low	192.168.2.1	Web application...	jQuery 1.4.2 <= 1.11.0 XSS Vulnerability
Low	192.168.2.1	General	Traceroute
Low	192.168.2.1	SSL and TLS	SSL/TLS: Report Supported Cipher Suites
Low	192.168.2.1	Service detection	SMB Remote Version Detection
Low	192.168.2.1	Service detection	CPE Inventory
Low	192.168.2.1	Windows	Microsoft Windows SMB Accessible Shares
Low	192.168.2.1	SSL and TLS	SSL/TLS: Report Medium Cipher Suites
Low	192.168.2.11	Service detection	HTTP Server type and version
Low	192.168.2.11	General	Relative IP Identification number change
Low	192.168.2.11	Service detection	Services
Low	192.168.2.11	Product detection	OS Detection Consolidation and Reporting
Low	192.168.2.11	Service detection	Hostname Determination Reporting
Low	192.168.2.11	Service detection	HTTP Server Banner Enumeration

3 STEP ATTACK



Automatically profile employees

Find passwords on the Dark Web

Break into your bank accounts

What could go wrong:

Using off-the-shelf marketing tools, criminals find your employees' details, then match them with credentials from the Dark Web. Armed with emails & passwords, they effortlessly access banking, email, and cloud services. This simple but effective method exposes your business to serious financial risks and data breaches.

Cyber Score Report

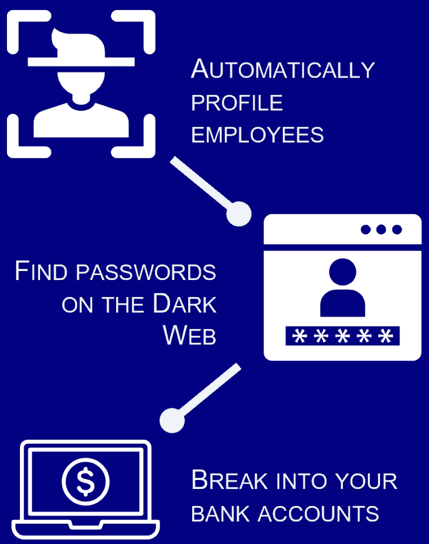
CASTILE SECURITY

Vulnerability Inventory

4/7 - All Monitored Risks

Priority	IP Address	Risk Family	Vulnerability
Low	192.168.2.11	Web application…	Web Application Scanning Consolidation / Info Reporting
Low	192.168.2.11	Web application…	HTTP Security Headers Detection
Low	192.168.2.11	General	Traceroute
Low	192.168.2.11	Service detection	CPE Inventory
Low	192.168.2.16	Product detection	OS Detection Consolidation and Reporting
Low	192.168.2.16	Service detection	Unknown OS and Service Banner Reporting
Low	192.168.2.16	Service detection	Hostname Determination Reporting
Low	192.168.2.16	General	Check open ports
Low	192.168.2.16	General	Traceroute
Low	192.168.2.12	Product detection	OS Detection Consolidation and Reporting
Low	192.168.2.12	Service detection	Hostname Determination Reporting
Low	192.168.2.12	General	Traceroute
Low	192.168.2.14	General	ICMP Timestamp Reply Information Disclosure
Low	192.168.2.14	Product detection	OS Detection Consolidation and Reporting
Low	192.168.2.14	Service detection	Hostname Determination Reporting
Low	192.168.2.14	General	Traceroute
Low	192.168.2.14	Service detection	CPE Inventory
Low	192.168.2.10	General	ICMP Timestamp Reply Information Disclosure
Low	192.168.2.10	Product detection	OS Detection Consolidation and Reporting
Low	192.168.2.10	Service detection	Hostname Determination Reporting

3 STEP ATTACK



Automatically profile employees

Find passwords on the Dark Web

Break into your bank accounts

What could go wrong:

Using off-the-shelf marketing tools, criminals find your employees' details, then match them with credentials from the Dark Web. Armed with emails & passwords, they effortlessly access banking, email, and cloud services. This simple but effective method exposes your business to serious financial risks and data breaches.

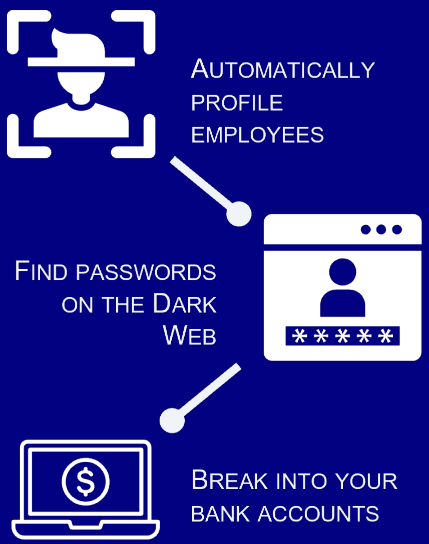
Cyber Score Report

Vulnerability Inventory

5/7 - All Monitored Risks

Priority	IP Address	Risk Family	Vulnerability
Low	192.168.2.10	General	Traceroute
Low	192.168.2.10	Service detection	CPE Inventory
Low	192.168.2.62	General	ICMP Timestamp Reply Information Disclosure
Low	192.168.2.62	Product detection	OS Detection Consolidation and Reporting
Low	192.168.2.62	Service detection	Hostname Determination Reporting
Low	192.168.2.62	General	Traceroute
Low	192.168.2.62	Service detection	CPE Inventory
Low	192.168.2.16	General	ICMP Timestamp Reply Information Disclosure
Low	192.168.2.16	Product detection	OS Detection Consolidation and Reporting
Low	192.168.2.16	Service detection	Hostname Determination Reporting
Low	192.168.2.16	General	Traceroute
Low	192.168.2.16	Service detection	CPE Inventory
Low	192.168.2.1	Service detection	HTTP Server type and version
Low	192.168.2.1	SSL and TLS	SSL/TLS: Certificate - Self-Signed Certificate Detection
Low	192.168.2.1	SSL and TLS	SSL/TLS: Certificate - Subject Common Name Does Not Match...
Low	192.168.2.1	General	ICMP Timestamp Reply Information Disclosure
Low	192.168.2.1	Service detection	Services
Low	192.168.2.1	SSL and TLS	SSL/TLS: Report Non Weak Cipher Suites
Low	192.168.2.1	SSL and TLS	SSL/TLS: Collect and Report Certificate Details
Low	192.168.2.1	Windows	SMB log in

3 STEP ATTACK



Automatically profile employees

Find passwords on the Dark Web

Break into your bank accounts

What could go wrong:

Using off-the-shelf marketing tools, criminals find your employees' details, then match them with credentials from the Dark Web. Armed with emails & passwords, they effortlessly access banking, email, and cloud services. This simple but effective method exposes your business to serious financial risks and data breaches.

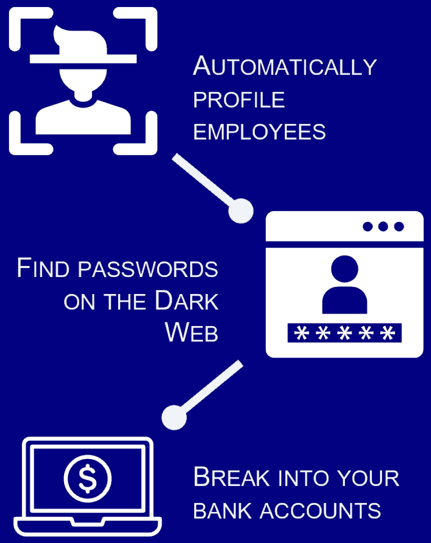
Cyber Score Report

Vulnerability Inventory

6/7 - All Monitored Risks

Priority	IP Address	Risk Family	Vulnerability
Low	192.168.2.1	SSL and TLS	SSL/TLS: Certificate Too Long Valid
Low	192.168.2.1	Windows	Check for Accessible Registry (Windows SMB Login)
Low	192.168.2.1	SSL and TLS	SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
Low	192.168.2.1	SSL and TLS	SSL/TLS: Version Detection
Low	192.168.2.1	SSL and TLS	SSL/TLS: HTTP Strict Transport Security (HSTS) Missing
Low	192.168.2.1	Product detection	OS Detection Consolidation and Reporting
Low	192.168.2.1	Service detection	DNS Server Detection (TCP)
Low	192.168.2.1	SSL and TLS	SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
Low	192.168.2.1	SSL and TLS	SSL/TLS: HTTP Public Key Pinning (HPKP) Missing
Low	192.168.2.1	SSL and TLS	SSL/TLS: HPKP / HSTS / Expect-CT Headers sent via plain HTTP
Low	192.168.2.1	Service detection	Unknown OS and Service Banner Reporting
Low	192.168.2.1	Service detection	Hostname Determination Reporting
Low	192.168.2.1	Windows	SMB Login Successful For Authenticated Checks
Low	192.168.2.1	Service detection	HTTP Server Banner Enumeration
Low	192.168.2.1	Service detection	SMB/CIFS Server Detection
Low	192.168.2.1	SSL and TLS	SSL/TLS: Hostname discovery from server certificate
Low	192.168.2.1	Web application…	Web Application Scanning Consolidation / Info Reporting
Low	192.168.2.1	Web application…	HTTP Security Headers Detection
Low	192.168.2.1	SSL and TLS	SSL/TLS: Safe/Secure Renegotiation Support Status
Low	192.168.2.1	SSL and TLS	SSL/TLS: Untrusted Certificate Detection

3 STEP ATTACK



Automatically profile employees

Find passwords on the Dark Web

Break into your bank accounts

What could go wrong:

Using off-the-shelf marketing tools, criminals find your employees' details, then match them with credentials from the Dark Web. Armed with emails & passwords, they effortlessly access banking, email, and cloud services. This simple but effective method exposes your business to serious financial risks and data breaches.

Cyber Score Report

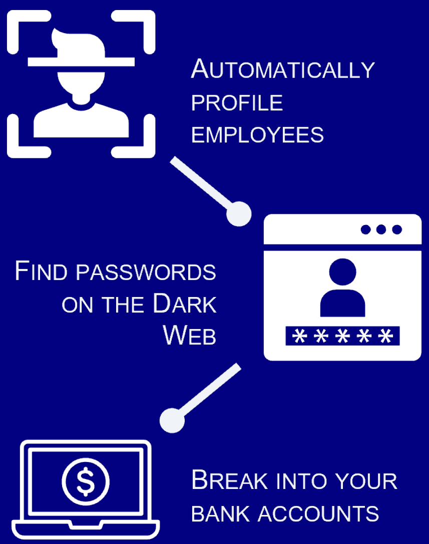
Vulnerability Inventory

7/7 - All Monitored Risks

Priority	IP Address	Risk Family	Vulnerability
Low	192.168.2.1	Service detection	SMBv1 Enabled - Active Check
Low	192.168.2.1	Web application...	jQuery < 3.0.0 XSS Vulnerability
Low	192.168.2.1	Web application...	jQuery < 1.9.0 XSS Vulnerability
Low	192.168.2.1	Web application...	jQuery < 3.4.0 Object Extensions Vulnerability
Low	192.168.2.1	Web application...	jQuery 1.2 < 3.5.0 XSS Vulnerability
Low	192.168.2.1	Web application...	jQuery < 1.9.0 XSS Vulnerability
Low	192.168.2.1	Product detection	jQuery Detection Consolidation
Low	192.168.2.1	Web application...	jQuery 1.4.2 <= 1.11.0 XSS Vulnerability
Low	192.168.2.1	General	Traceroute
Low	192.168.2.1	SSL and TLS	SSL/TLS: Report Supported Cipher Suites
Low	192.168.2.1	Service detection	SMB Remote Version Detection
Low	192.168.2.1	Service detection	CPE Inventory
Low	192.168.2.1	Windows	Microsoft Windows SMB Accessible Shares
Low	192.168.2.1	SSL and TLS	SSL/TLS: Report Medium Cipher Suites

CASTILE SECURITY

3 STEP ATTACK



Automatically profile employees

Find passwords on the Dark Web

Break into your bank accounts

What could go wrong:

Using off-the-shelf marketing tools, criminals find your employees' details, then match them with credentials from the Dark Web. Armed with emails & passwords, they effortlessly access banking, email, and cloud services. This simple but effective method exposes your business to serious financial risks and data breaches.