

Spending a lot of Money and still getting Hacked?

A professionally evil approach can be your BFF.



Jordan Bonagura
jordan.bonagura@secureideas.com

secureideas.com



professionally evil®

Jordan Bonagura

Senior Security Consultant

OVER 25 YEAR OF INDUSTRY EXPERIENCE

Senior Security Consultant / Penetration Tester

College Professor and course coordinator

Worked on encryption of satellite communication

Worked with police crime-solving unit

Used to be a CISO

JORDAN.BONAGURA@SECUREIDEAS.COM

Copyright © 2026 Secure Ideas LLC

Agenda

- Information Value
- The Chronic Myopia
- Pseudo Security
- The Data Doesn’t Lie
- Same Crime, New Stats
- Real World Examples
- And Now?
- Q&A

Copyright © 2026 Secure Ideas LLC



Information Value

Copyright © 2026 Secure Ideas LLC

Importance of your company data.

Let's reflect on the IMPORTANCE of your company data.



- What type of data do you have?
- How many data do you have?
- How important is it?

Copyright © 2026 Secure Ideas LLC

Importance of your company data.

WHAT IF you need

company **WITHOUT**





Copyright © 2026 Secure Ideas LLC

SecureIdeas professionally evil®

Importance

Even worse, what i

INTO WRONG HA





Copyright © 2026 Secure Ideas LLC

SecureIdeas professionally evil®

Importance of your company data.

So, knowing that your information is so important, why don't you take care of it?



Copyright © 2026 Secure Ideas LLC

Importance o





BUT I AM!

I have the best equipm

vendors, and tools!

Copyright © 2026 Secure Ideas LLC

SecureIdeas professionally evil®

Importance of your company data.

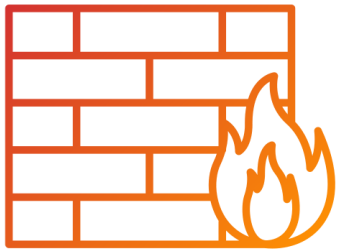
WE HAVE CONTROLS!

Physical Controls



Locks!

Logical Controls



Firewall, IDS/IPS, A.V. etc

Services



Policies and Standards



Lockpicking Tools



Criminals



Users

She couldn't access her Facebook account at work anymore...

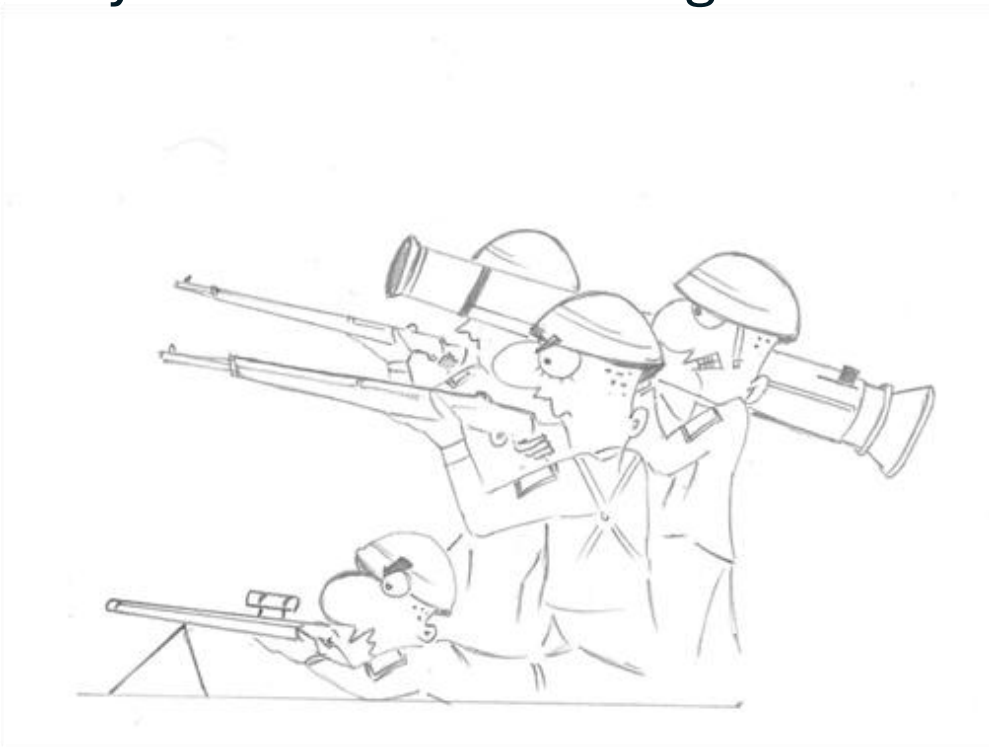
Copyright © 2026 Secure Ideas LLC

Importance of your company data.

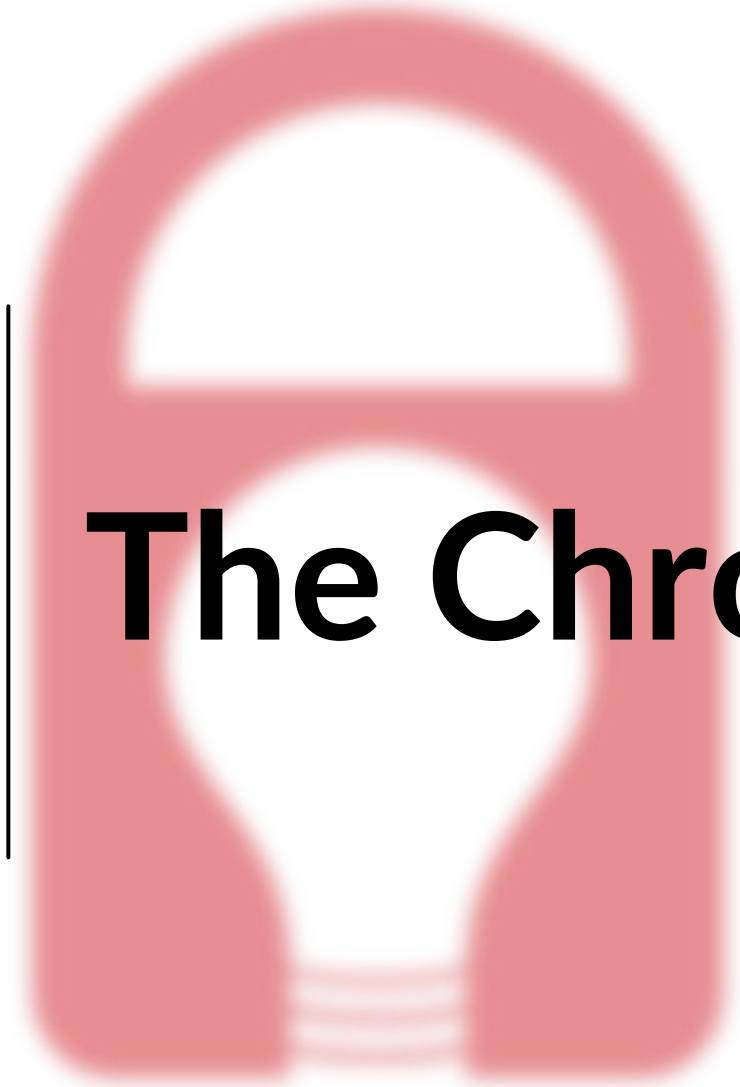
We also have a **CISO!**

- Seeking solutions for security triad – aka C.I.A.
- Enterprise risk management.
- Understanding, mitigating and trying to stay ahead of a wide range of risks
- People Management





Copyright © 2026 Secure Ideas LLC

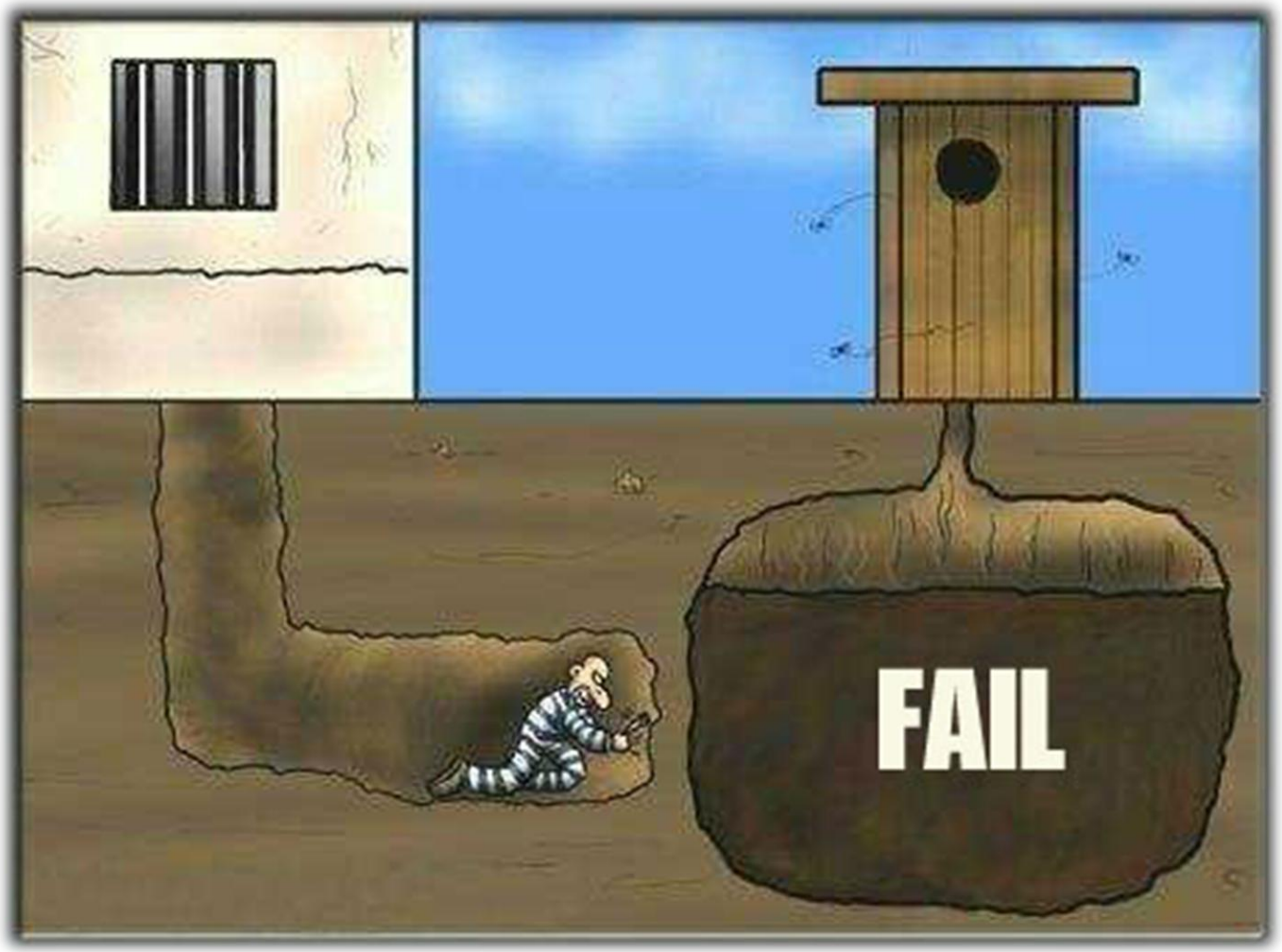


The Chronic Myopia

Copyright © 2026 Secure Ideas LLC

The Chronic Myopia

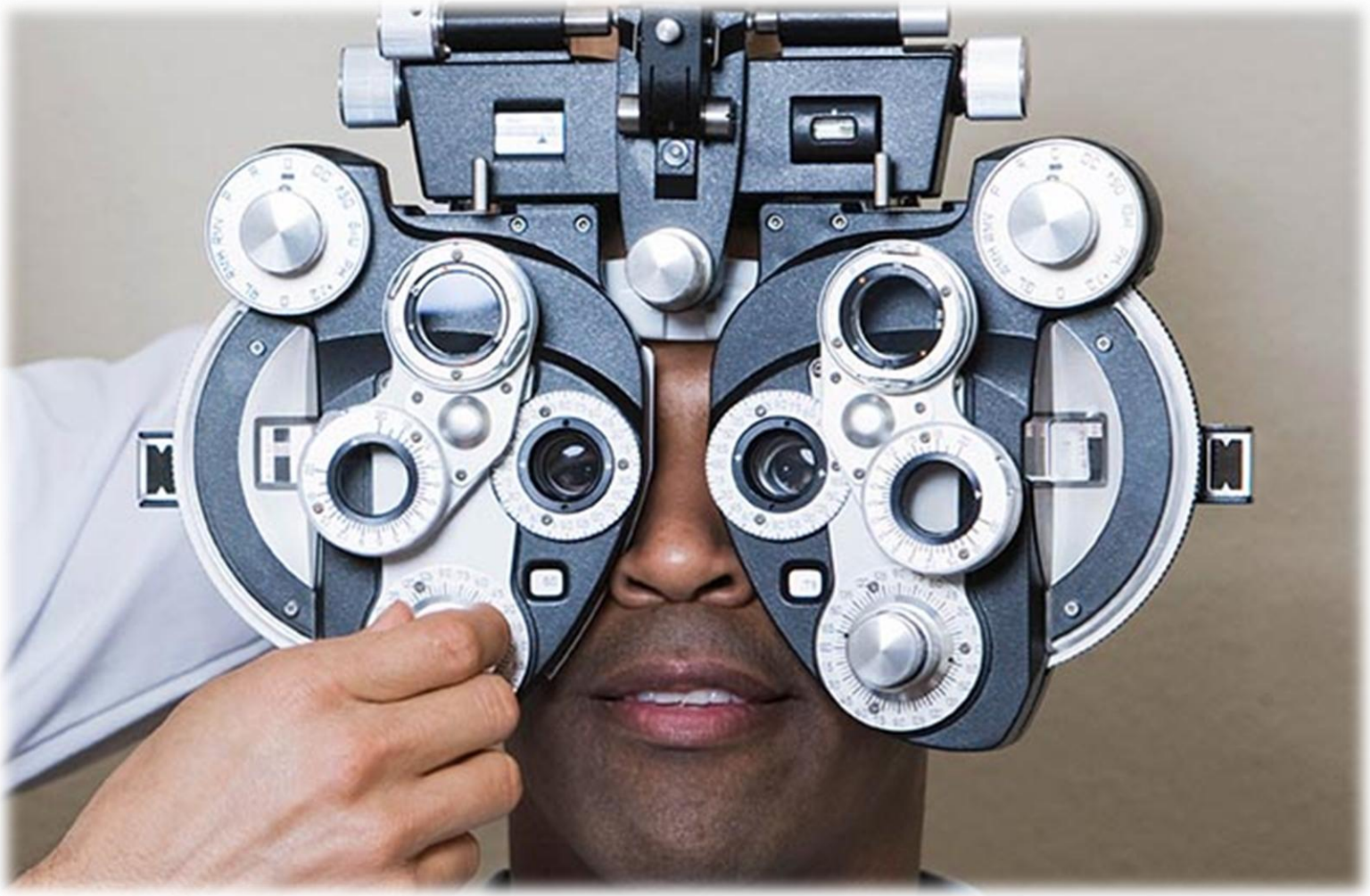
Problem solved?



Copyright © 2026 Secure Ideas LLC

The Chronic Myopia

An Eye Exam



Copyright © 2026 Secure Ideas LLC





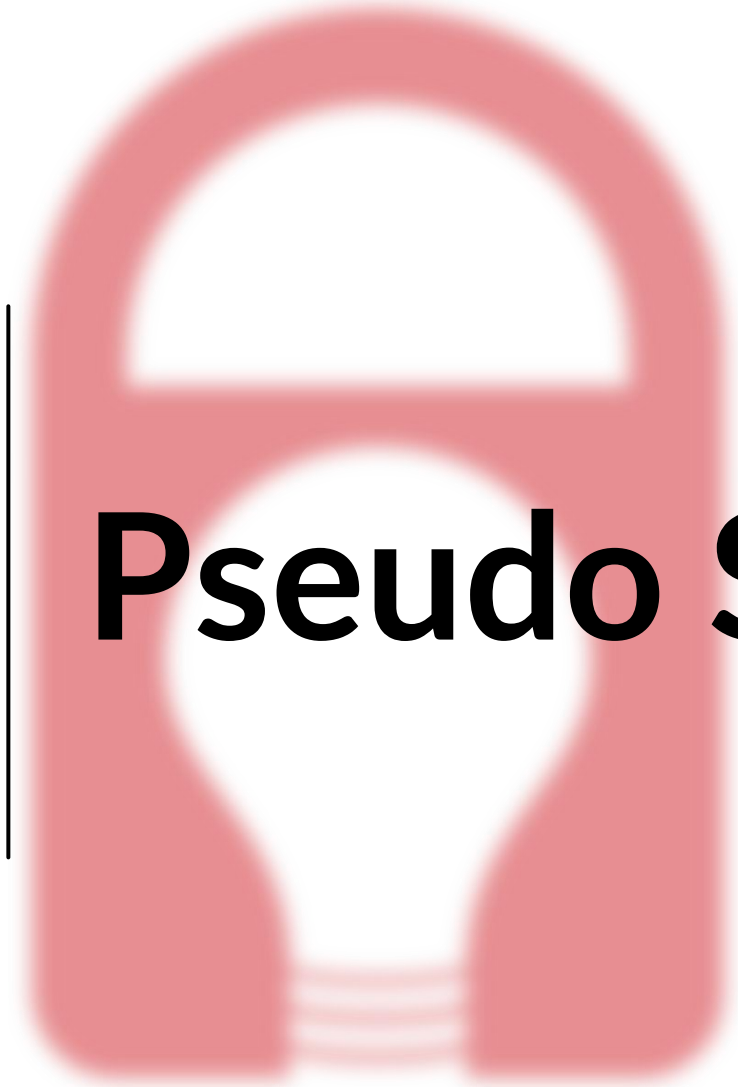


The Chronic Myopia





Copyright © 2026 Secure Ideas LLC



Pseudo Security

Copyright © 2026 Secure Ideas LLC

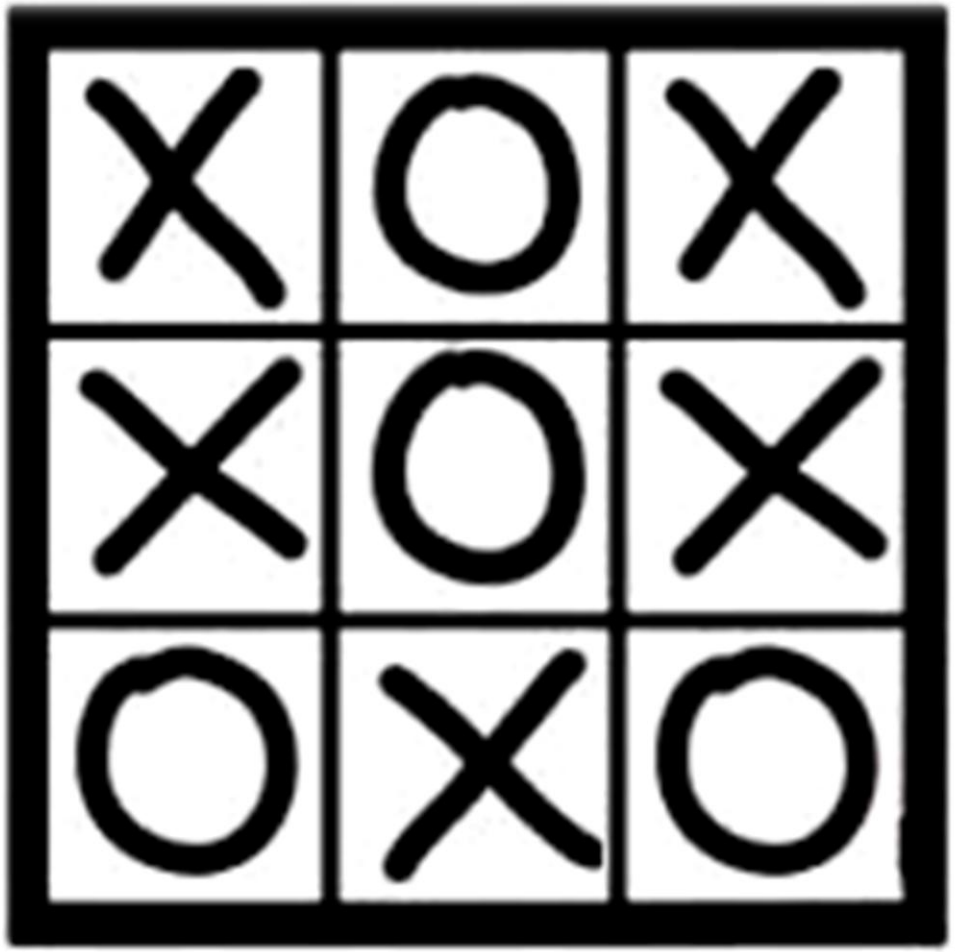
Importance of your company data.



Copyright © 2026 Secure Ideas LLC

Pseudo Security

CAN YOU WIN?

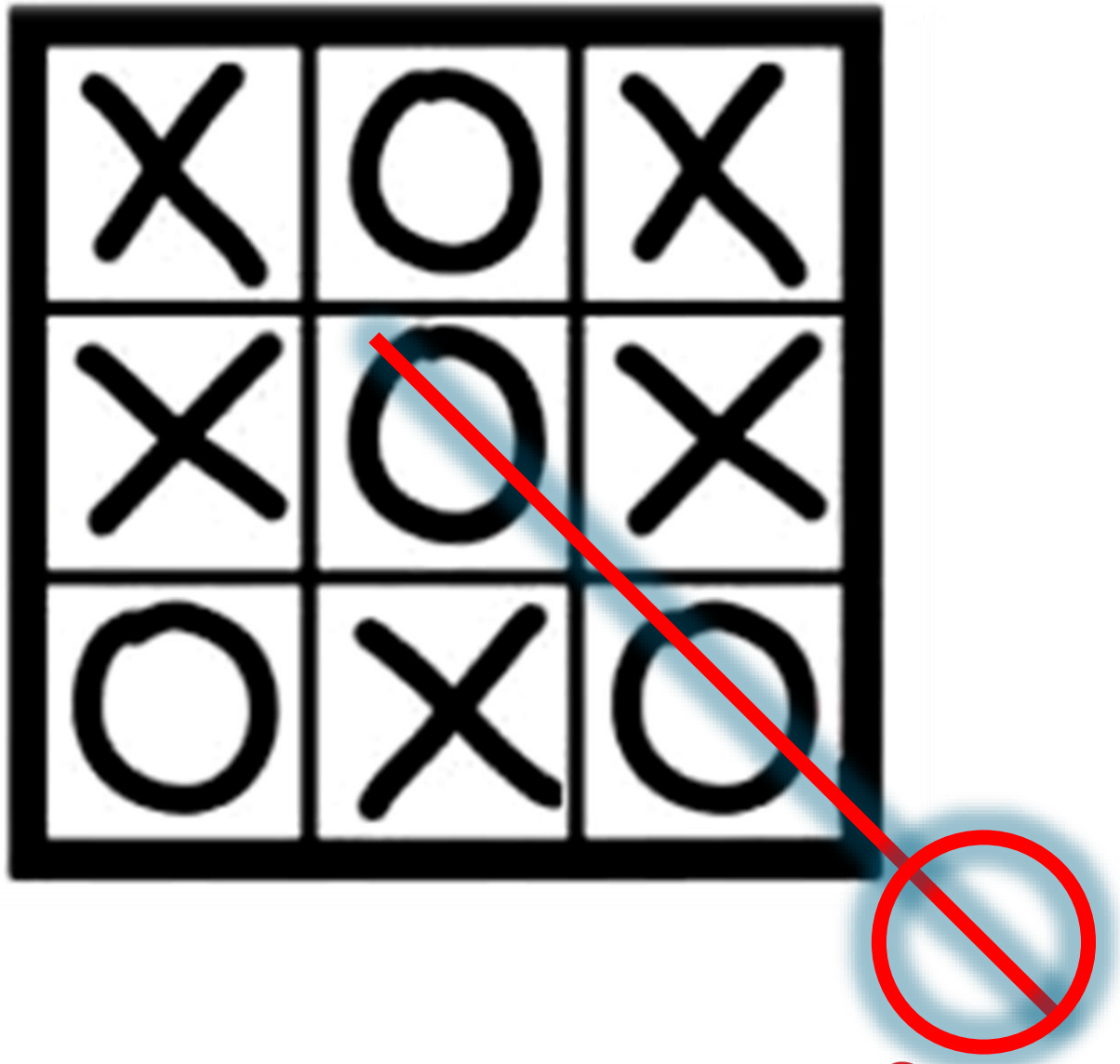


Copyright © 2026 Secure Ideas LLC

Pseudo Security

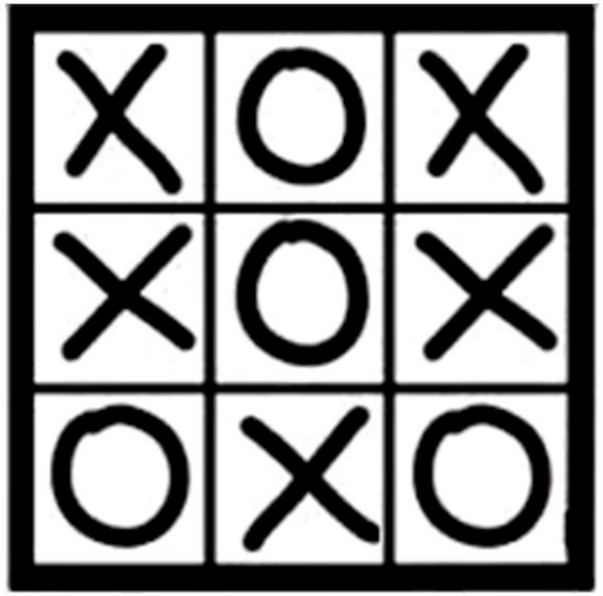
BREAKING NEWS!!!

CRIMINALS do not follow your rules and policies…



Copyright © 2026 Secure Ideas LLC

Pseudo Security



Copyright © 2026 Secure Ideas LLC

Pseudo Security

HOW DO CRIMINALS THINK?

There are NO RULES, or rather, there are, but not for those who want to break it…

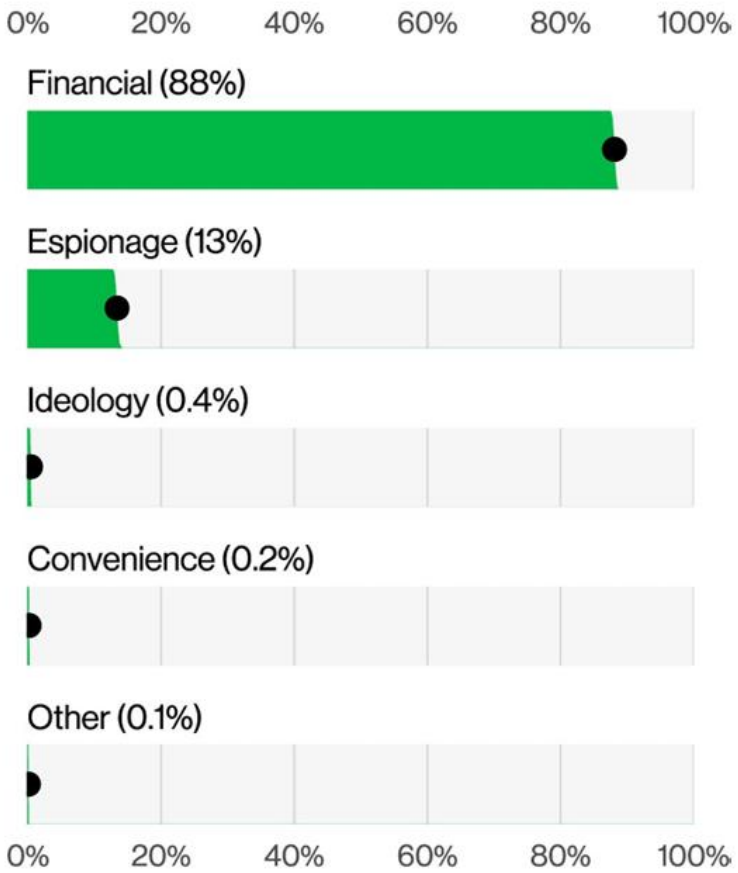


Figure 25. Top actor Motives in breaches (n=18,175)

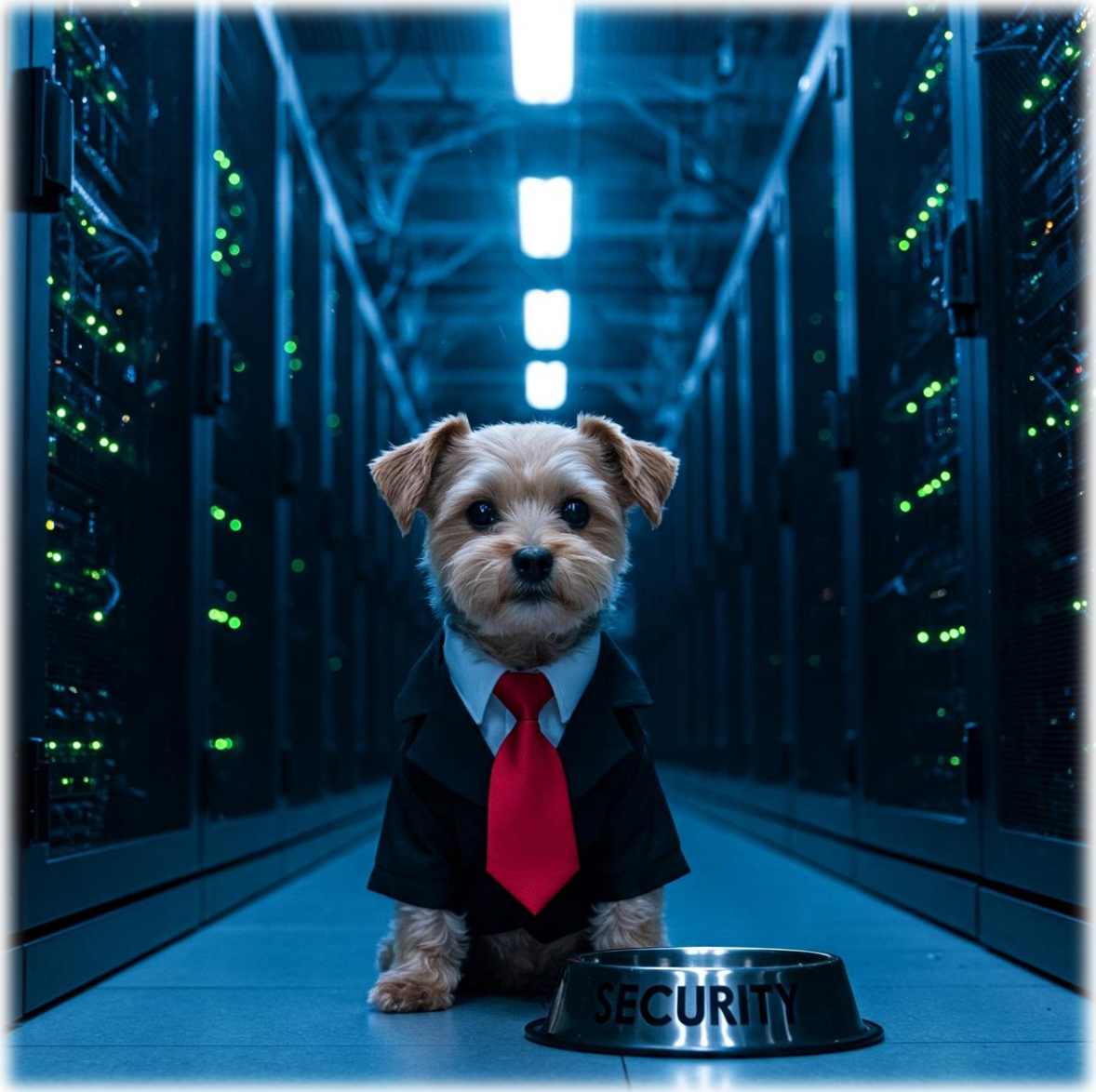
Source: Verizon DBIR 2026

Copyright © 2026 Secure Ideas LLC

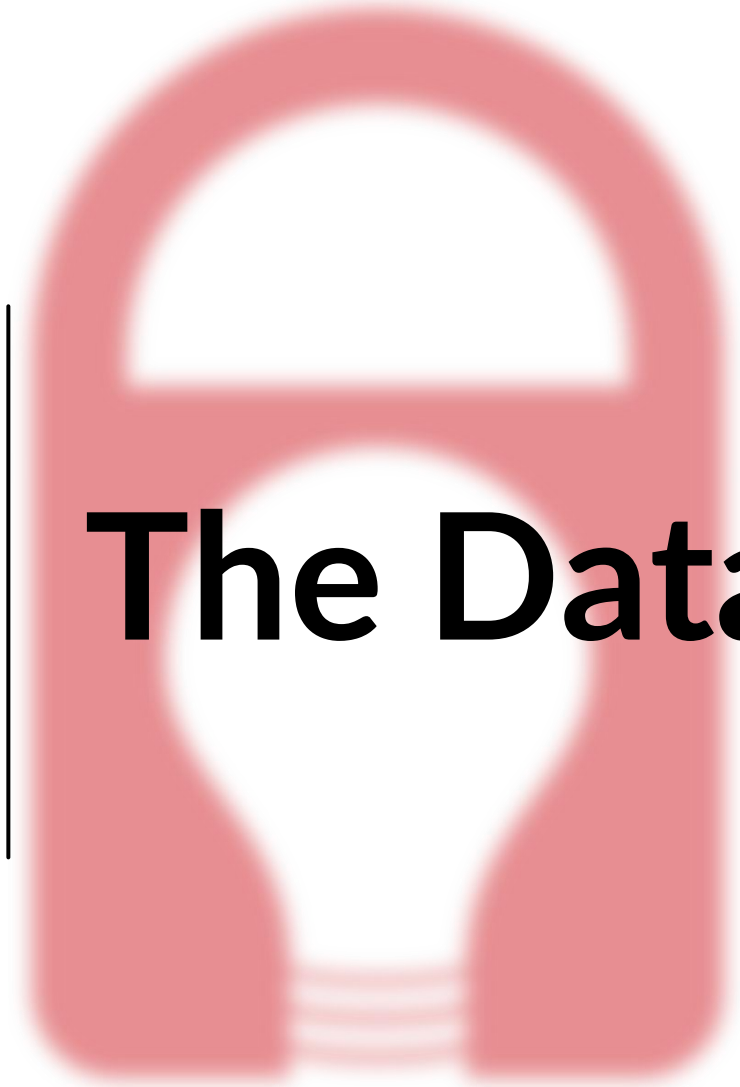
Pseudo Security

NOT ON MY COMPANY!!!

Supported by your OWN policies, you become prisoner of a PSEUDO SECURITY.



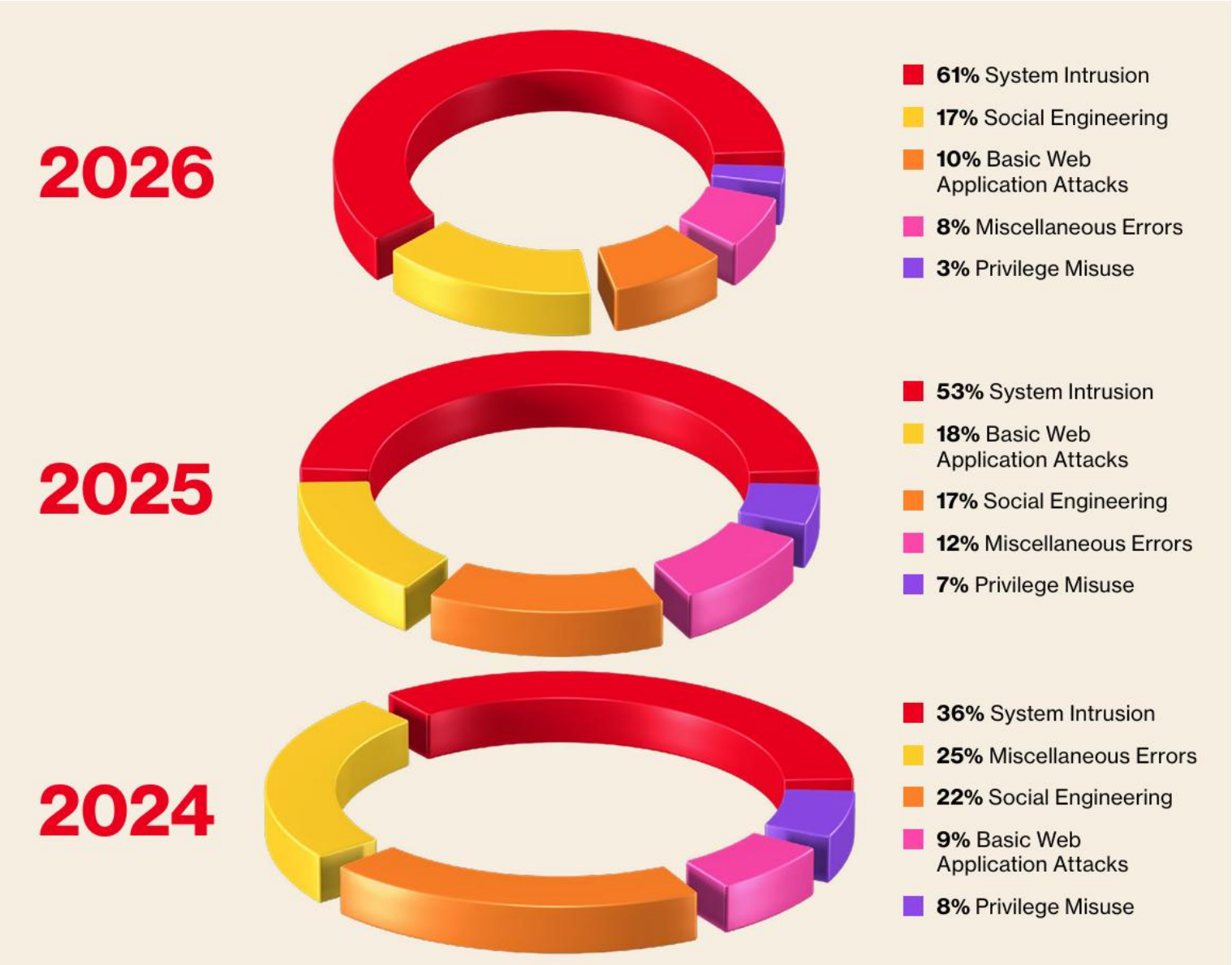
Copyright © 2026 Secure Ideas LLC



The Data Doesn't Lie

Copyright © 2026 Secure Ideas LLC

The Data Doesn't Lie



Source: Verizon DBIR 2026

Copyright © 2026 Secure Ideas LLC

SecureIdeas professionally evil®

The Data Doesn't Lie

	Incidents			
Industry	Total	Small (1–1,000)	Large (1,000+)	Unknown
Total	31,861	7,257	528	24,076
Accommodation (72)	319	89	11	219
Administrative (56)	422	295	12	115
Agriculture (11)	223	34	0	189
Construction (23)	843	525	8	310
Education (61)	1,302	219	22	1,061
Entertainment (71)	587	90	5	492
Finance (52)	3,809	365	52	3,392
Healthcare (62)	1,492	472	21	999
Information (51)	1,703	214	79	1,410
Management (55)	103	30	0	73
Manufacturing (31–33)	3,627	1,198	56	2,373
Mining (21)	72	35	3	34
Other Services (81)	900	206	4	690
Professional (54)	3,578	1,400	82	2,096
Public Administration (92)	3,634	148	17	3,469
Real Estate (53)	505	189	1	315
Retail (44–45)	997	315	32	650
Transportation (48–49)	689	242	24	423
Utilities (22)	638	57	8	573
Wholesale (42)	1,057	877	18	162
Unknown	5,361	257	73	5,031
Total	31,861	7,257	528	24,076

Table 3. Number of security incidents by victim industry and organization size

Source: Verizon DBIR 2026

Copyright © 2026 Secure Ideas LLC

SecureIdeas professionally evil®

Same Crime, New Stats

Initial access vector – Changed Leaders

2025

- **Stolen Creds → 22-32%**
- **Vulnerability Exploitation → 18-20%**

2026

- **Vulnerability Exploitation → 31%**
- **Stolen Creds → 13%**

Patching

2025 → 38% - Median time 32 days

2026 → 26% - Median time 43 days

Human Element

2025 → 60%

2026 → 62%

Third Parties!

2025 → 30%

2026 → 48%

Source: Verizon DBIR 2026

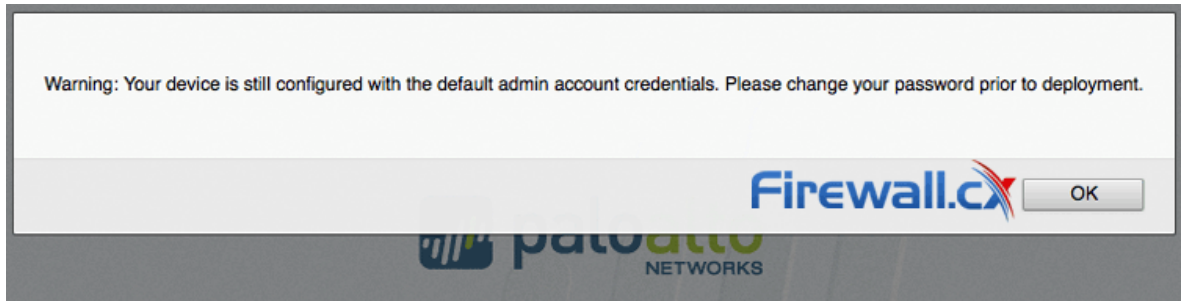
Copyright © 2026 Secure Ideas LLC

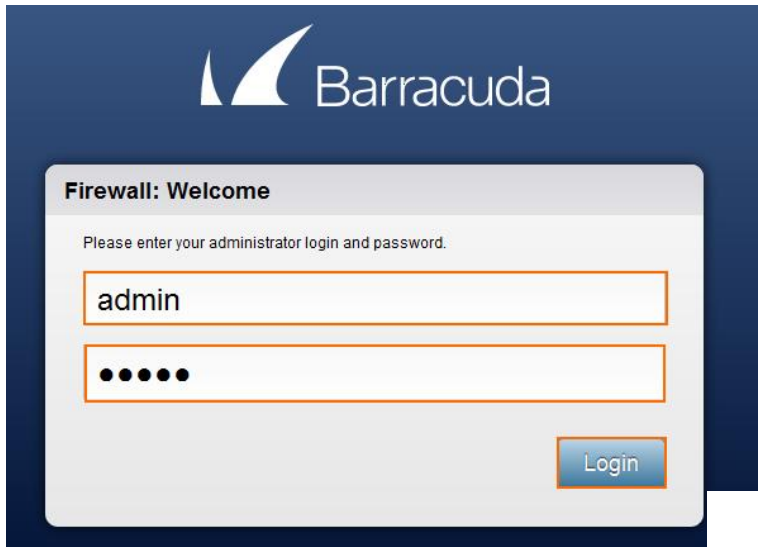


Real World Examples

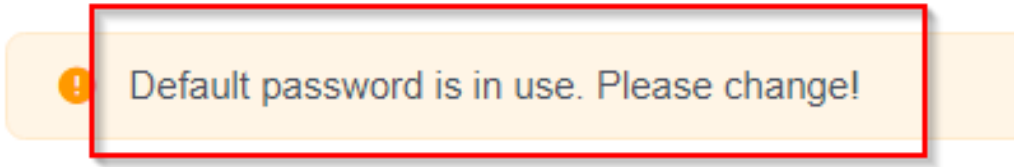
Copyright © 2026 Secure Ideas LLC

Default Credentials



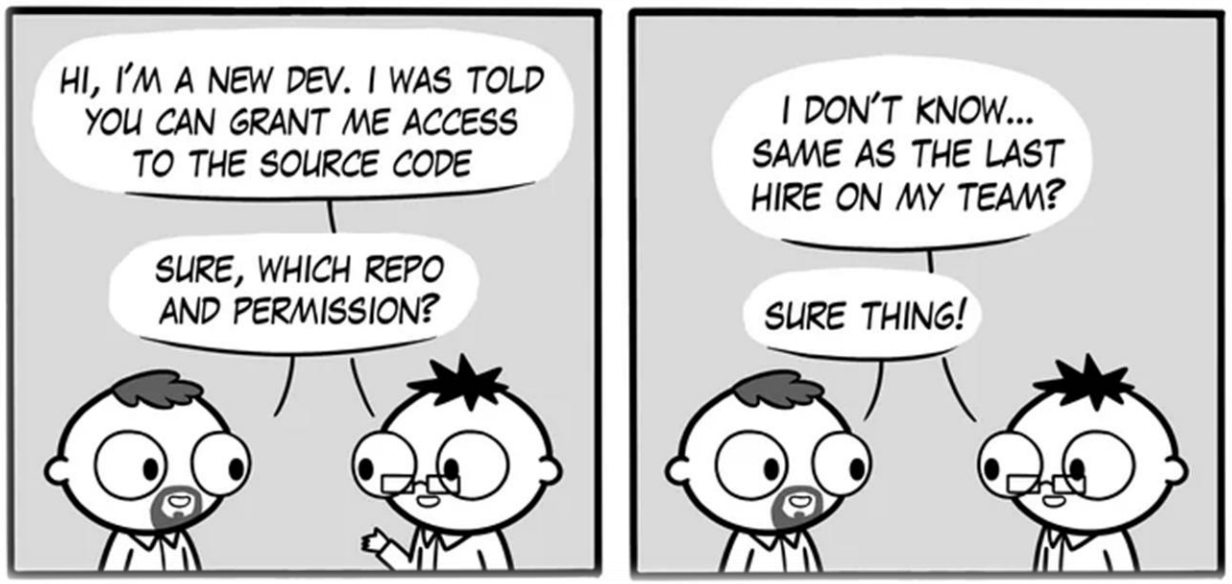






Copyright © 2026 Secure Ideas LLC

Developer is NOT an Admin!

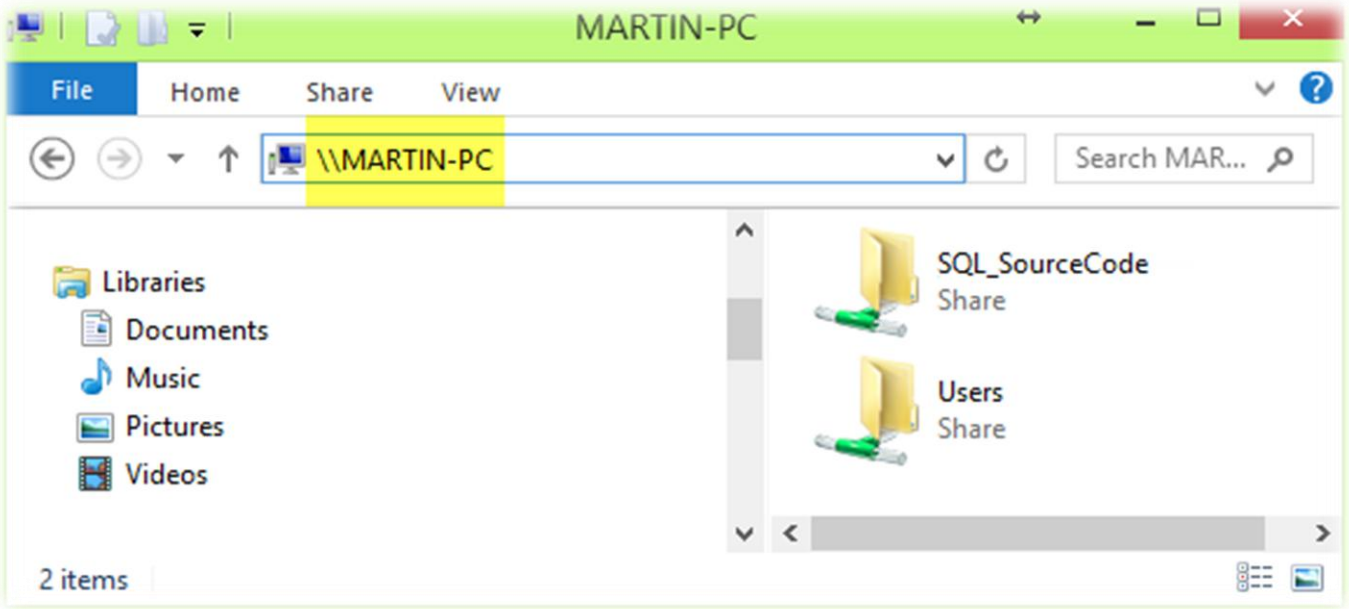


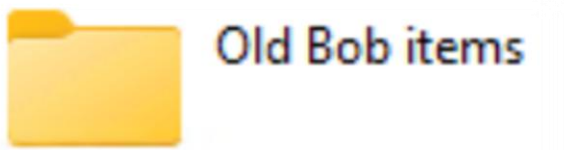


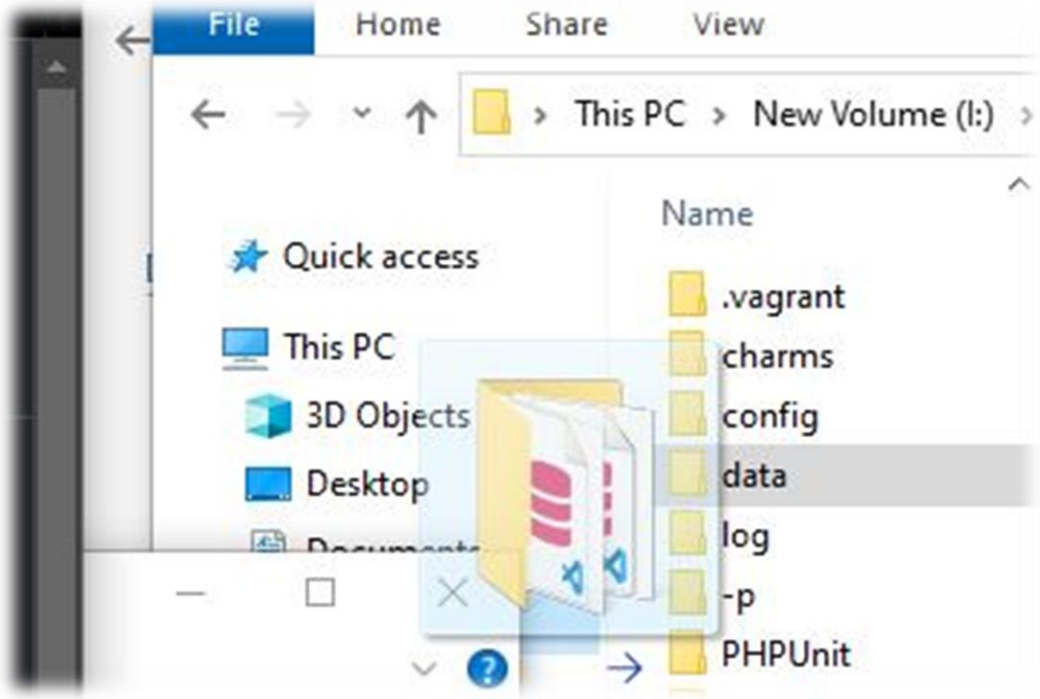
Principle of Least Privilege.

Copyright © 2026 Secure Ideas LLC

File Shares Containing Sensitive Data







Copyright © 2026 Secure Ideas LLC

Use of EOL Software



Copyright © 2026 Secure Ideas LLC

SecureIdeas professionally evil®

Use of Unencrypted Protocols

```
└─$ telnet [redacted]
Trying [redacted]
Connected to [redacted]
Escape character is '^]'.


Hello... connected to ipIO-X!
Connected to Telnet Session 3


User> admin
Password> *****

ipIO-X> help
```

```
└─$ ftp [redacted]
Connected to [redacted]
220----------------------------------------------------------------------
220-This is the "Banner" message for the Mac OS X Server's FTP server process.
220-
220-              FTP clients will receive this message immediately
220-              before being prompted for a name and password.
220-
220-PLEASE NOTE:
220-
220-       Some FTP clients may exhibit problems if you make this file too long.
220-
220----------------------------------------------------------------------
220-
220 [redacted]FTP server ready.
```


Copyright © 2026 Secure Ideas LLC

SecureIdeas professionally evil®

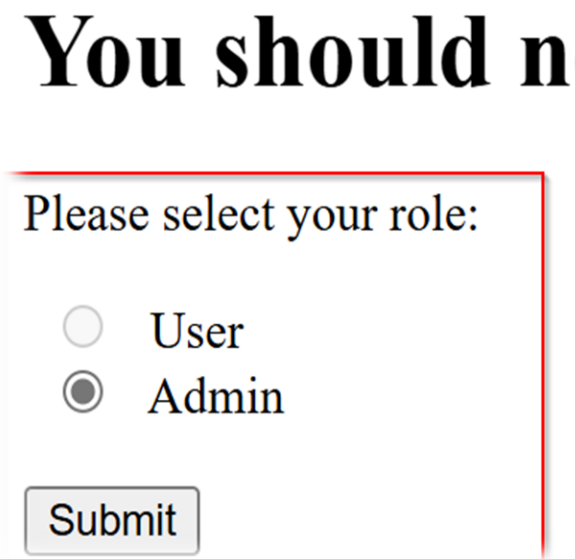
Lack of Backend Protection




```
<input type="radio" id="html" name="fav_language" value="User"
checked="true" disabled>
"   "
<label for="html">User</label>
<br>
"   "
<input type="radio" id="css" name="fav_language" value="Admin"
disabled>
"   "
<label for="css">Admin</label>
<br>
"   "
<br>
<input type="submit" value="Submit" disabled> == $0
```


Copyright © 2026 Secure Ideas LLC
SecureIdeas professionally evil®

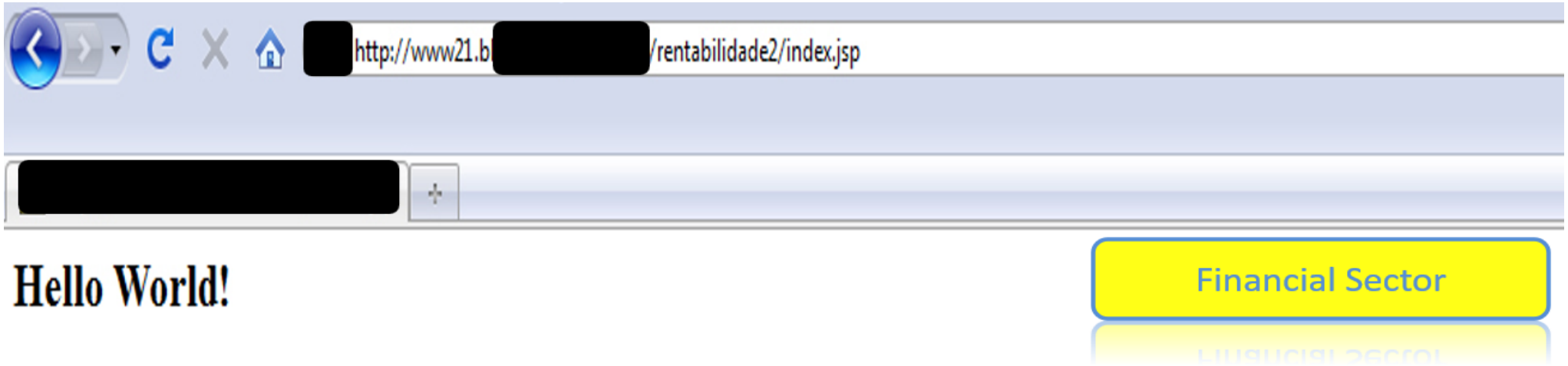
Lack of Backend Protection




```
<p>Please select your role:</p>
"   "
<input type="radio" id="html" name="fav_language" value="User"
disabled>
"   "
<label for="html">User</label>
<br>
"   "
<input type="radio" id="css" name="fav_language" value="Admin">
"   "
<label for="css">Admin</label>
<br>
"   "
<br>
<input type="submit" value="Submit"> == $0
```


Copyright © 2026 Secure Ideas LLC
SecureIdeas professionally evil®

Testing in Production



Let's start with:

"HELLO WORLD!"

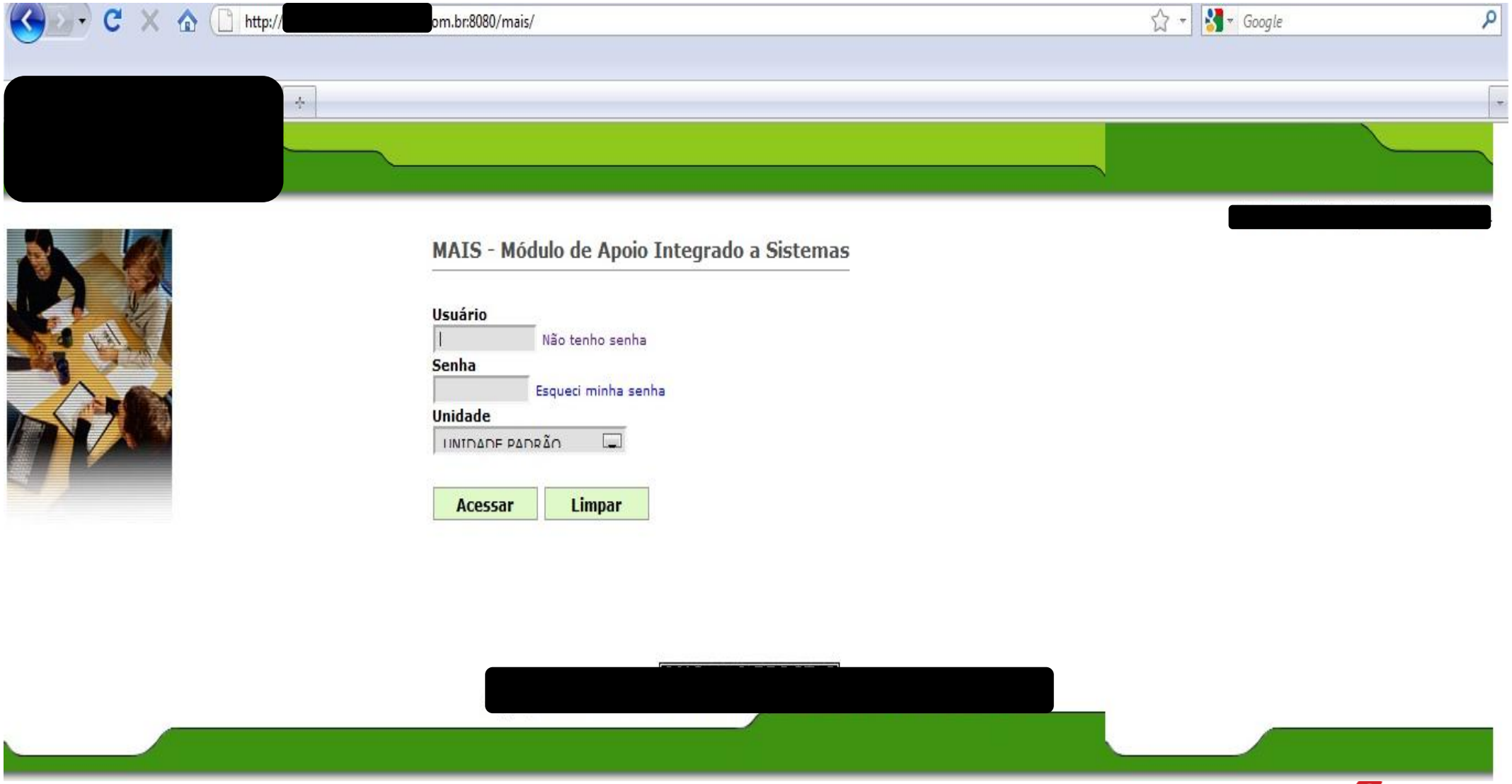
Copyright © 2026 Secure Ideas LLC

Renamed backend files



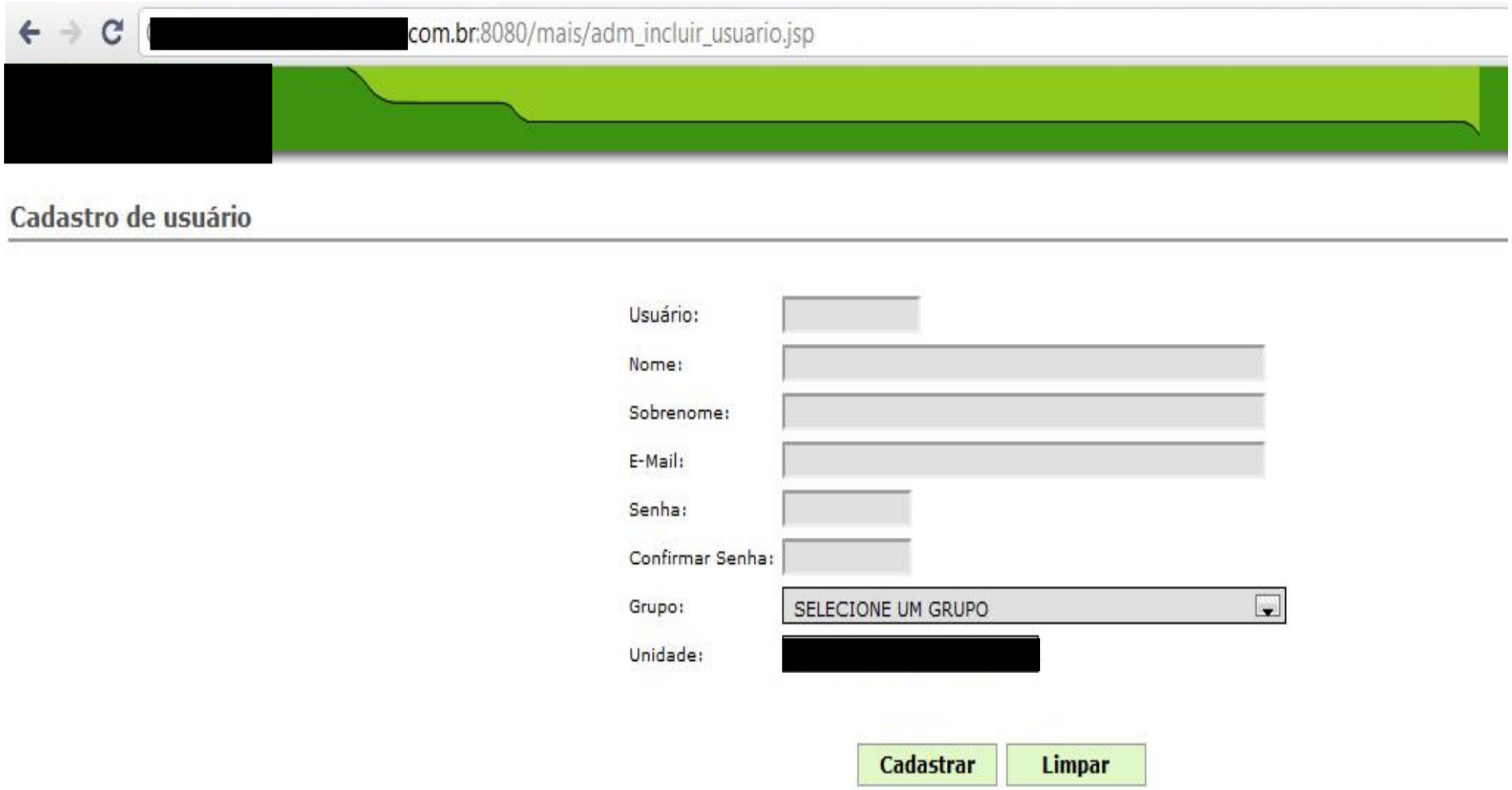
Copyright © 2026 Secure Ideas LLC

Ineffective Security Control



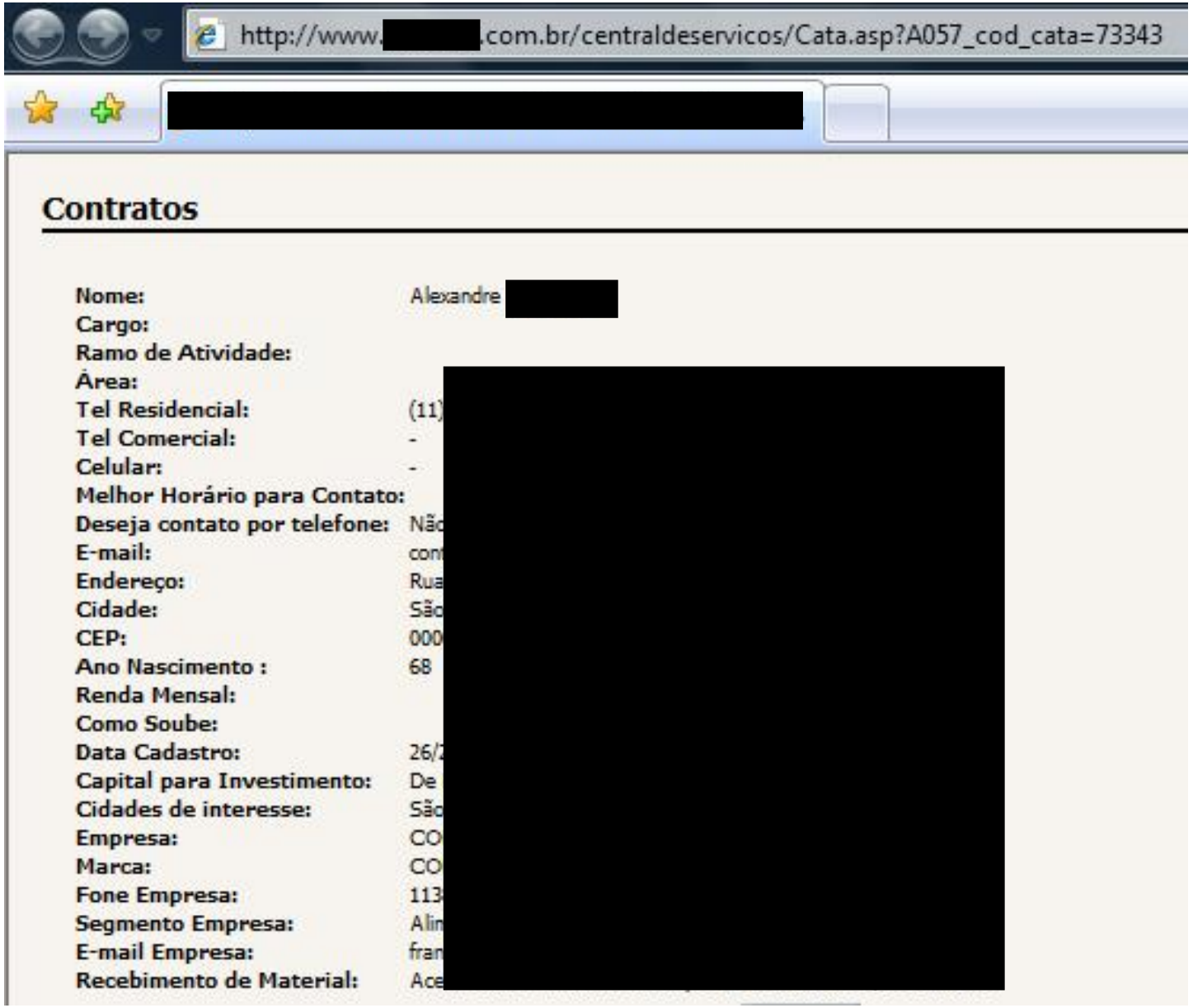
Copyright © 2026 Secure Ideas LLC

Ineffective Security Control



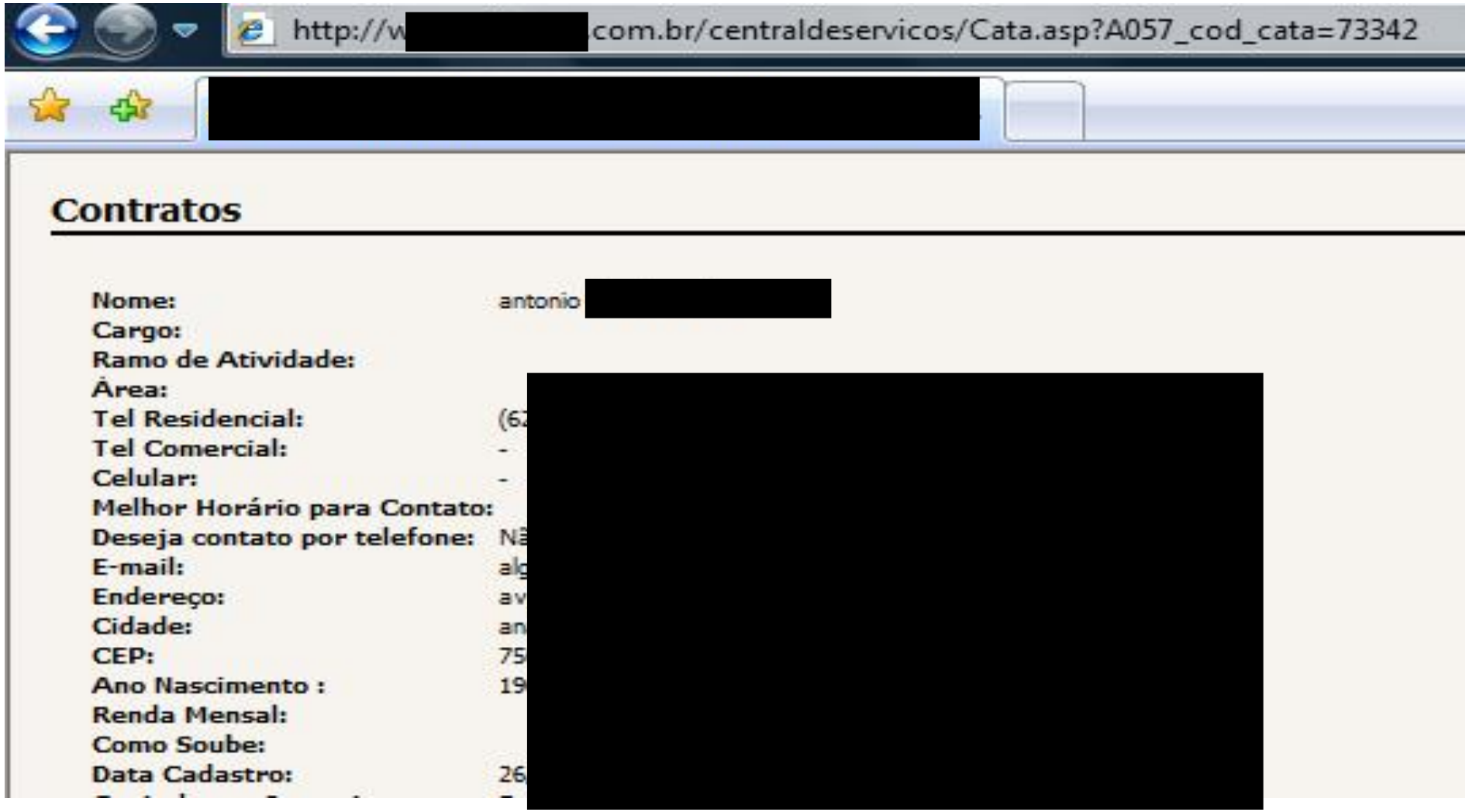
Copyright © 2026 Secure Ideas LLC

IDOR



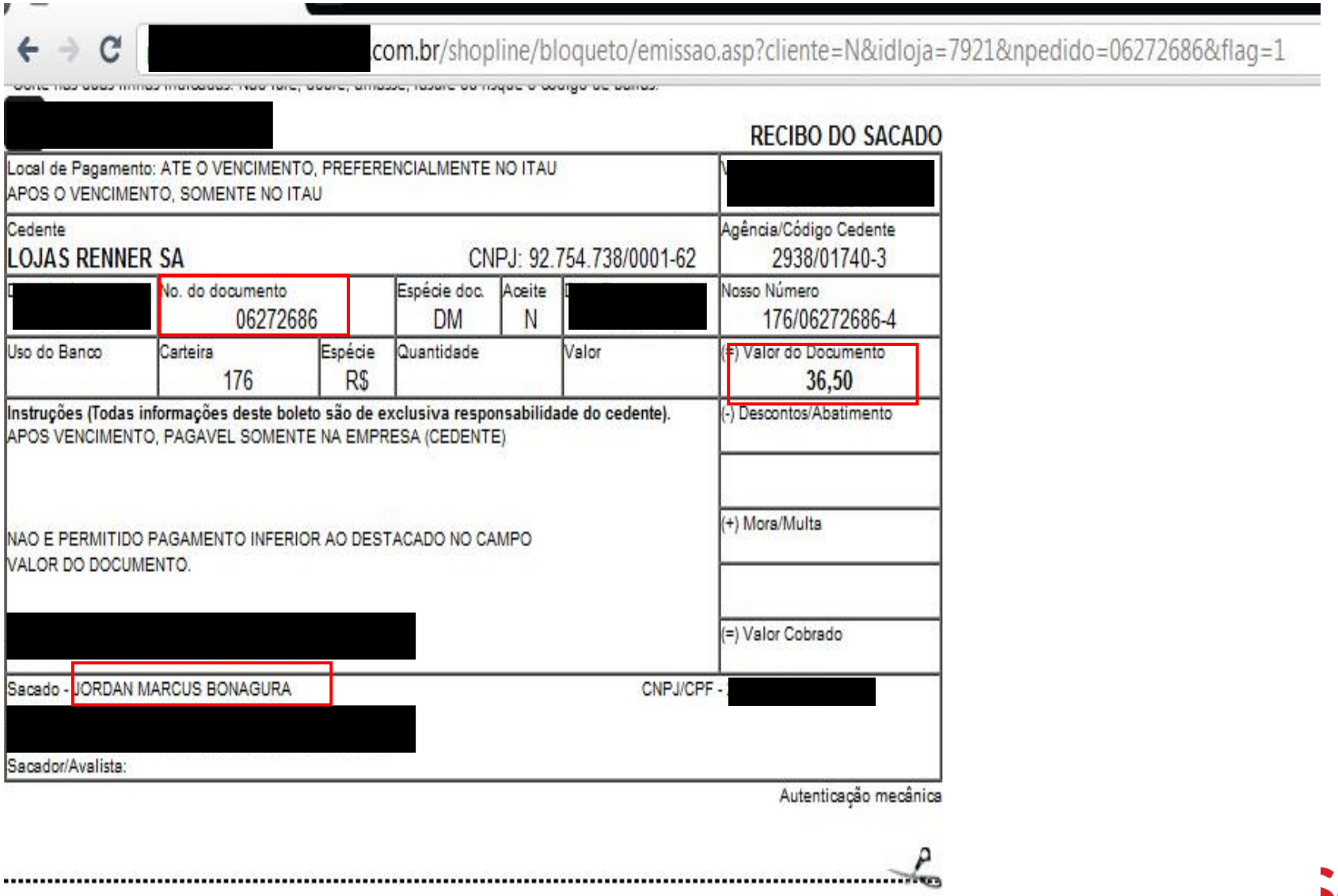
Copyright © 2026 Secure Ideas LLC

IDOR



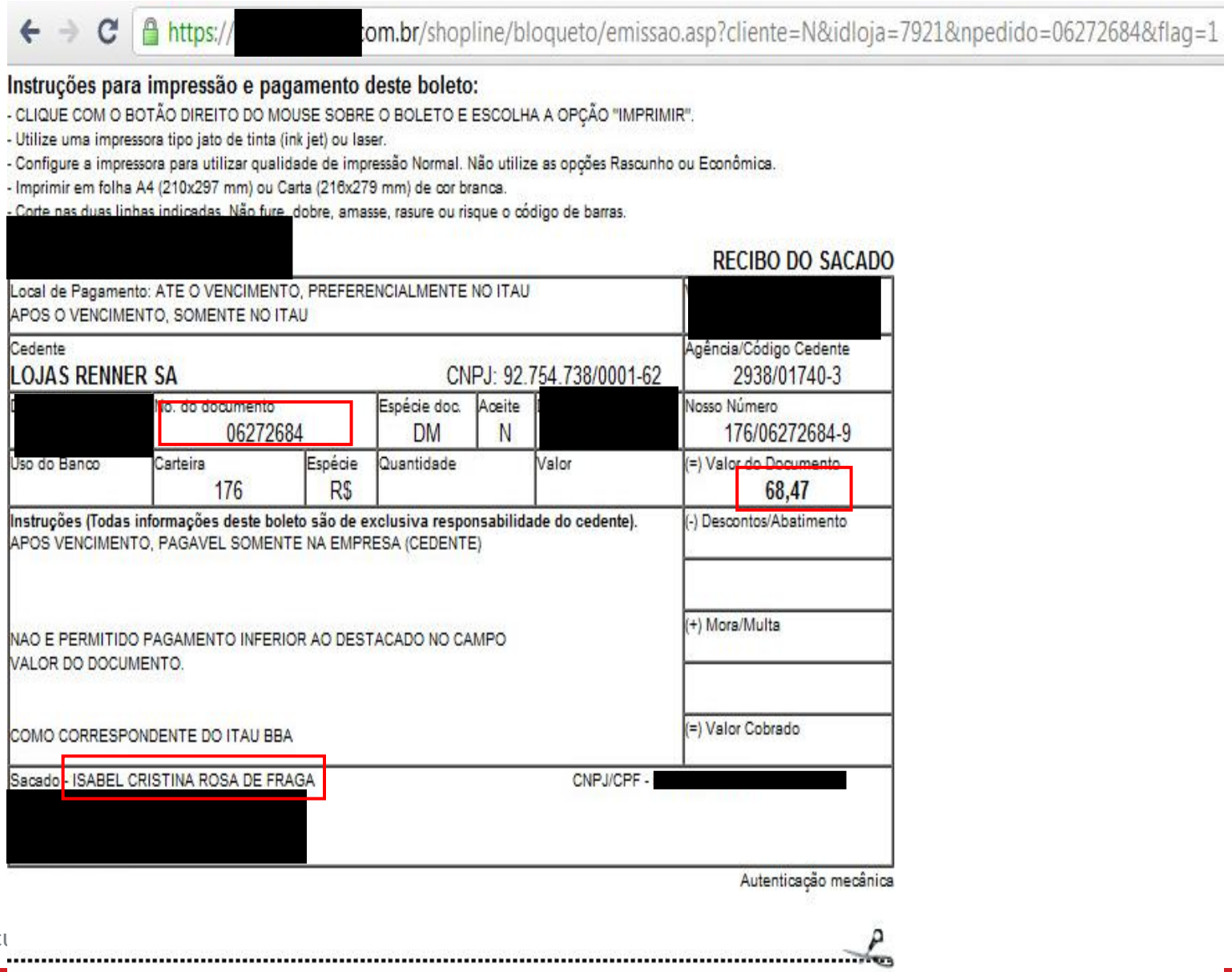
Copyright © 2026 Secure Ideas LLC

IDOR



Copyright © 2026 Secure Ideas LLC

IDOR


https://[redacted]com.br/shopline/bloqueto/emissao.asp?cliente=N&idloja=7921&npedido=06272684&flag=1

Instruções para impressão e pagamento deste boleto:

- CLIQUE COM O BOTÃO DIREITO DO MOUSE SOBRE O BOLETO E ESCOLHA A OPÇÃO "IMPRIMIR".
- Utilize uma impressora tipo jato de tinta (ink jet) ou laser.
- Configure a impressora para utilizar qualidade de impressão Normal. Não utilize as opções Rascunho ou Econômica.
- Imprimir em folha A4 (210x297 mm) ou Carta (216x279 mm) de cor branca.
- Corte nas duas linhas indicadas. Não fure, dobre, amasse, rasure ou risque o código de barras.

[redacted]

RECIBO DO SACADO

Local de Pagamento: ATE O VENCIMENTO, PREFERENCIALMENTE NO ITAU APOS O VENCIMENTO, SOMENTE NO ITAU					[redacted]
Cedente LOJAS RENNER SA			CNPJ: 92.754.738/0001-62		Agência/Código Cedente 2938/01740-3
[redacted]	Nro. do documento 06272684	Espécie doc. DM	Aceite N	[redacted]	Nosso Número 176/06272684-9
Uso do Banco	Carteira 176	Espécie R$	Quantidade	Valor	(=) Valor do Documento 68,47
Instruções (Todas informações deste boleto são de exclusiva responsabilidade do cedente). APOS VENCIMENTO, PAGAVEL SOMENTE NA EMPRESA (CEDENTE) NAO E PERMITIDO PAGAMENTO INFERIOR AO DESTACADO NO CAMPO VALOR DO DOCUMENTO. COMO CORRESPONDENTE DO ITAU BBA					(-) Descontos/Abatimento (+) Mora/Multa (=) Valor Cobrado
Sacado - ISABEL CRISTINA ROSA DE FRAGA [redacted]			CNPJ/CPF - [redacted]		

Autenticação mecânica

Copyright © 2026 Secu

SecureIdeas professionally evil®

Leaked Credentials

```
└─$ nxc smb 10.0.200.20 -u usernames.txt -p passwords.txt -x 'net localgroup administrators'
SMB         10.0.200.20     445    WORKSTATION03    [*] Windows 10 / Server 2019 Build 19041 x64 (name:WORKSTATION03) (domain:milkyway.local) (
e) (SMBv1:False)
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\larry:password123 STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\steve:password123 STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\stationx-admin:password123 STATUS_LOGON_FAILURE
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\larry:passwords STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\steve:passwords STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\stationx-admin:passwords STATUS_LOGON_FAILURE
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\larry:Password123! STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [-] milkyway.local\steve:Password123! STATUS_NO_LOGON_SERVERS
SMB         10.0.200.20     445    WORKSTATION03    [+] milkyway.local\stationx-admin:Password123! (Pwn3d!)
SMB         10.0.200.20     445    WORKSTATION03    [+] Executed command via wmiexec
SMB         10.0.200.20     445    WORKSTATION03    Alias name     administrators
SMB         10.0.200.20     445    WORKSTATION03    Comment        Administrators have complete and unrestricted access to the computer/domain
SMB         10.0.200.20     445    WORKSTATION03    Members
SMB         10.0.200.20     445    WORKSTATION03    -------------------------------------------------------------------------------
SMB         10.0.200.20     445    WORKSTATION03    adam
SMB         10.0.200.20     445    WORKSTATION03    Administrator
SMB         10.0.200.20     445    WORKSTATION03    milkyway\Domain Admins
SMB         10.0.200.20     445    WORKSTATION03    The command completed successfully.
```


Copyright © 2026 Secure Ideas LLC



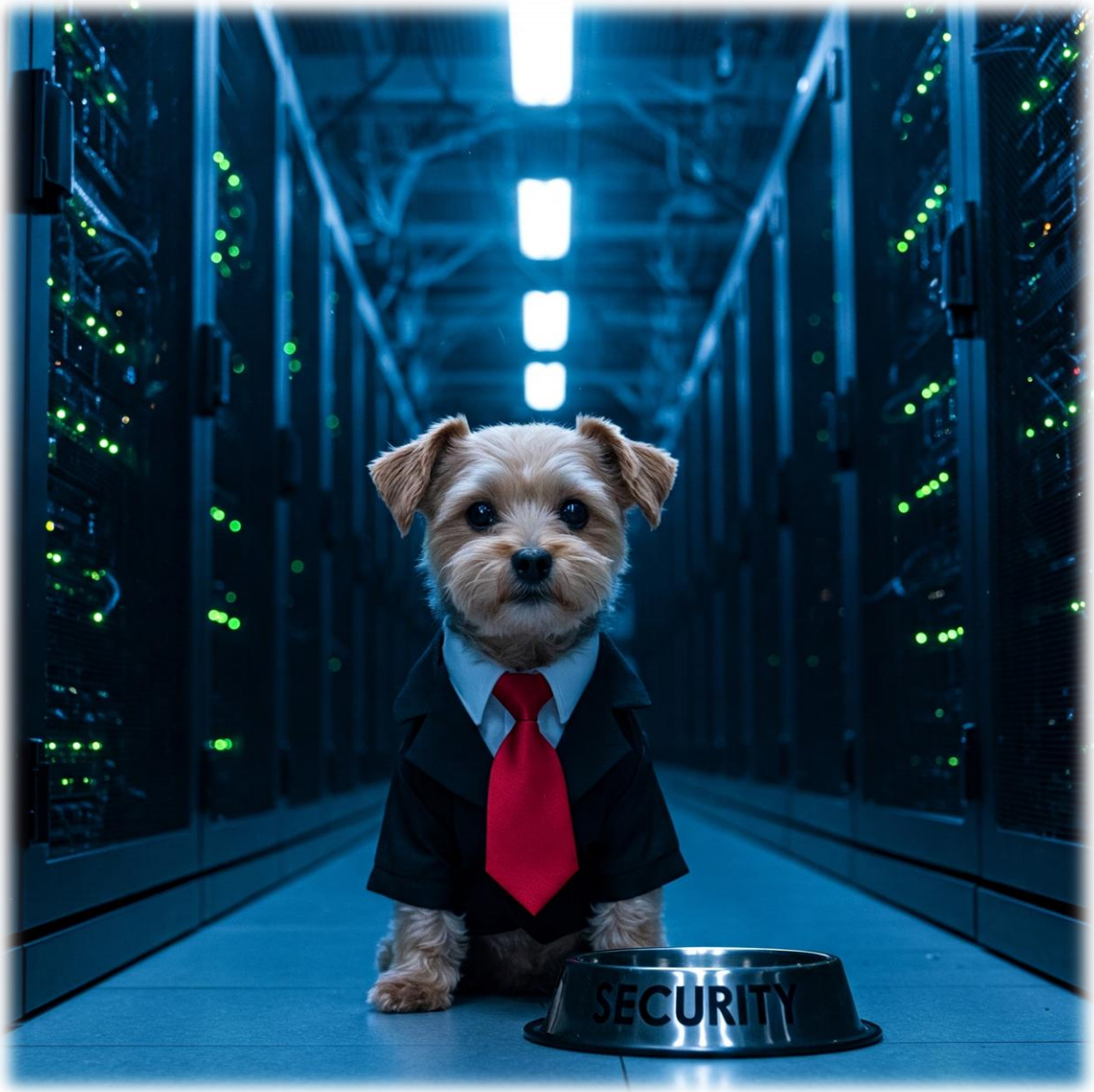
And Now?

Copyright © 2026 Secure Ideas LLC

Easy… Thanks!

Thanks, I GOT IT!

I need to review my EOL, open files shares, permissions, default creds, etc, right?



Symptoms are NOT the same than root cause

Copyright © 2026 Secure Ideas LLC

Failed Attempts

SECURITY

You CAN N

LAPTOP.



Copyright © 2026 Secure Ideas LLC

SecureIdeas professionally evil®

Let's think!



Copyright © 2026 Secure Ideas LLC

Let's think!



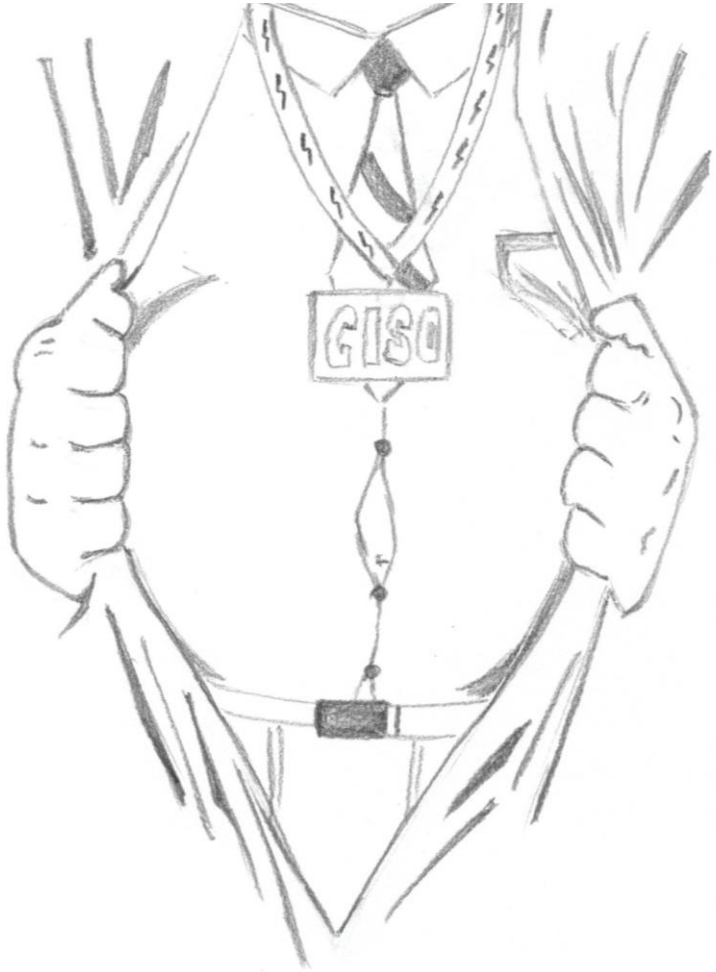


Copyright © 2026 Secure Ideas LLC

Let's think!

This is a mission for the **Super CISO**





Being a Super CISO means understanding that a superhero doesn't need to act on everything.

The most important quality is to have an open mind and be willing to ask for help and check to see what the market is already providing.

Copyright © 2026 Secure Ideas LLC

What is necessary?

- What is necessary?

An outside perspective.



Specialized professionals and companies can offer more **impartial, less biased views.**

Copyright © 2026 Secure Ideas LLC

“An outside perspective can help alleviate problems rooted in habitual tunnel vision.”

Jordan Bonagura



“We can’t fix it if we never face it!”

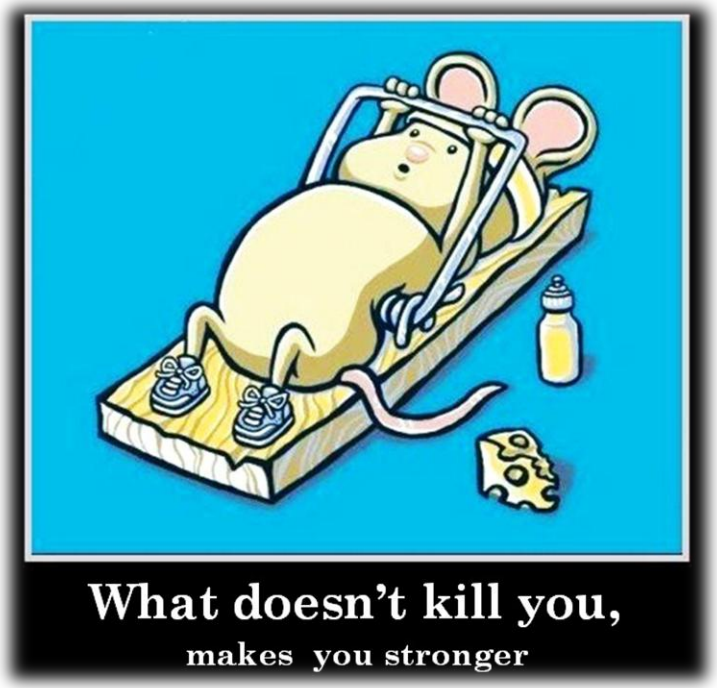


K POP DEMON HUNTERS – RUMI

Additional Resources

CIS Critical Security Controls (https://www.cisecurity.org/controls/v8-1)

- Establishing Essential Cyber Hygiene
- CIS Controls Cloud Companion Guide
- Guide to Enterprise Assets and Software
- CIS Benchmarks List



Verizon DBIR (Data Breach Investigations Report)

- https://www.verizon.com/business/resources/Td15/reports/2026-dbir-data-breach-investigations-report.pdf

Copyright © 2026 Secure Ideas LLC

QUESTIONS?

ISSA
Information Systems Security Association
Central Florida Chapter





jordan.bonagura@secureideas.com

Copyright © 2026 Secure Ideas LLC