IT NATION™ SECURE

hosted by CONNECTWISE®

Best of Both Worlds: Privileged Access Management

Presented by: Wes Spencer VP, Cybersecurity Strategy, CyberFOX

IT NATION™ SECURE

Wes Spencer

Professional:

- Based in Tampa, FL
- VP, Cybersecurity Strategy, CyberFOX
- Founder, CEO Empath Cyber
- Cybersecurity expert and co-founder of Perch Security
- Former (recovering) bankster – CIO at FNB Bank
- Chairman of FS-ISAC CIC – Cyber threat sharing group of 4,000+ banks and credit unions
- 2020 National Cybersecurity Educator of the Year

Personal:

- I run a YouTube channel of 80k subs on cybersecurity + crypto + startups
- Super duper into bourbon and cryptocurrency (not at the same time)
- I play too much Minecraft with the kids

Right from the ancient manuscripts

"Most security-related training courses and documentation discuss the implementation of a principle of least privilege, **yet organizations rarely follow it.** The **principle is simple**, and the impact of applying it correctly **greatly increases your security and reduces your risk**. The principle states that all users should log on with a user account that has the absolute minimum permissions necessary to complete the current task and nothing more."

The Administrator Accounts Security Planning Guide, 1999

Right from the ancient manuscripts

"Always think of security in terms of granting the least amount of privileges required to carry out the task. If an application that has too many privileges should be compromised, the attacker might be able to expand the attack beyond what it would if the application had been under the least amount of privilege.”.

Microsoft Windows Security Resource Kit, 1995

Stepping into the modern age

"The principles described in the preceding excerpts have not changed, but in assessing Active Directory installations, we invariably find excessive numbers of accounts that have been granted rights and permissions far beyond those required to perform day-to-day work."

Implementing Least-Privilege Administrative Models, 2023

Stepping into the modern age

Neither broad privilege nor deep privilege is necessarily dangerous, but when many accounts in the domain are **permanently granted broad and deep privilege**, if only one of the accounts is compromised, it can quickly be used to **reconfigure the environment to the attacker's purposes** or even to destroy large segments of the infrastructure.

Implementing Least-Privilege Administrative Models, 2023

The latest from Verizon DBIR

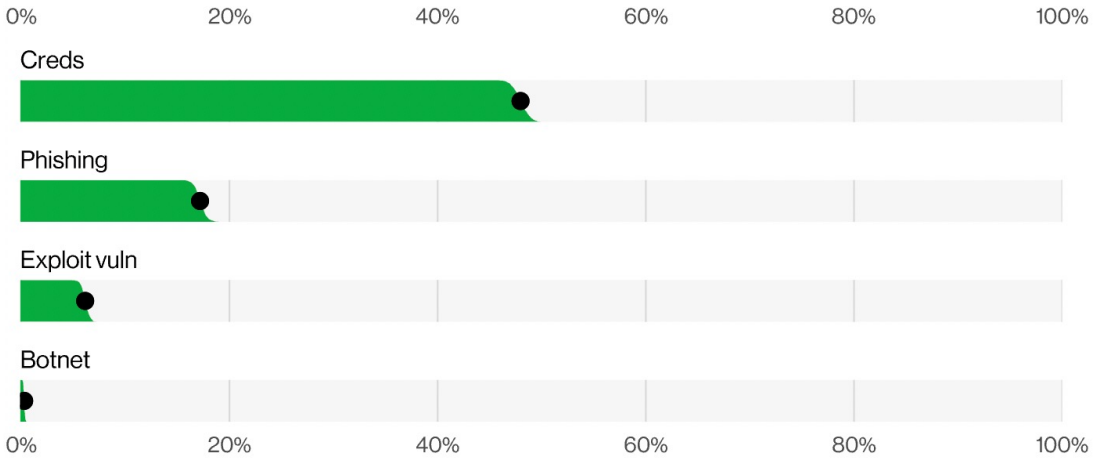


Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

There are four key paths leading to your estate: Credentials, Phishing, Exploiting vulnerabilities, and Botnets. All four are pervasive in all areas of the DBIR, and no organization is safe without a plan to handle each of them.

The latest from Verizon DBIR

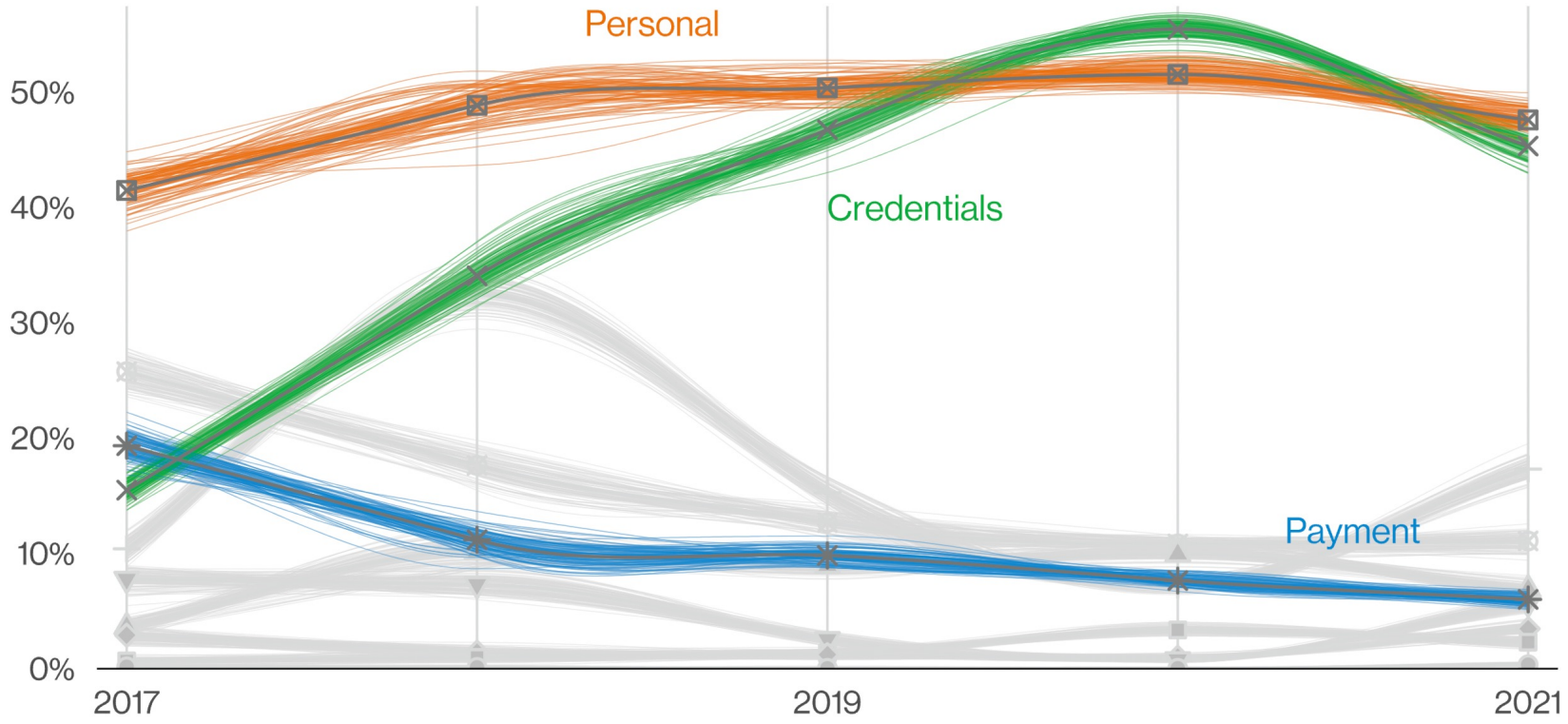


Figure 27. Top confidentiality varieties over time in breaches

Privilege escalation attacks

Exploit misconfigurations

Bugs

Weak passwords

Other system vulnerabilities

Privilege escalation attacks

Over 90%

of Windows breaches are successful because users have privileged access (80% of those are compromised passwords)

Removing user admin rights mitigates

94%

of all critical Microsoft vulnerabilities

CIS Critical Security Controls where PAM helps

Control 4: Secure Configuration of Enterprise Assets and Software

4.7 Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.

Control 5: Account Management

5.1 Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

CIS Critical Security Controls where PAM helps

Control 5: Account Management

5.2 Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.

5.4 Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

5.5 Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

CIS Critical Security Controls where PAM helps

Control 6: Access Control Management

A modern PAM Solution will assist with:

6.1 Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.

6.2 Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

6.7 Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.

6.8 Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

What does cyber insurance say?

h.	Do you manage privileged accounts using privileged account management software (e.g., CyberArk, BeyondTrust, etc.)? **If "Yes", please provide the name of your provider:** _____	☐ Yes ☐ No
i.	Do you actively monitor all administrator access for unusual behavior patterns? **If "Yes", please provide the name of your monitoring tool:** _____	☐ Yes ☐ No

12. Do you have a process for managing computer accounts, including the removal of outdated access accounts in a timely fashion? ☐ Yes ☐ No

14. Do you have access control procedures that address access to critical and sensitive computer systems? ☐ Yes ☐ No

Directory, Domains, and Accounts

11. Do you have a formal **Identity and Access Management** programme in place? ☐ Yes ☐ No

12. How many privileged users have full access to your directory service, including your **Active Directory Domain**?

13. How many users have persistent administrative access to workstations and servers other than their own?

14. How many total number of users have administrative access?

17. Have you disabled all local administrative accounts? ☐ Yes ☐ No

a. If no, please provide details on how this is managed:

The kill chain

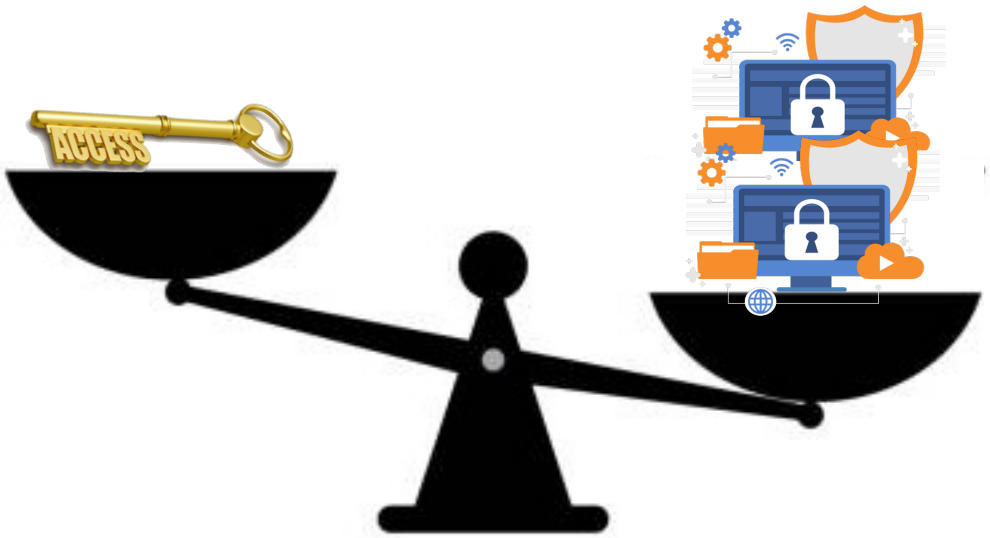
Best Practices According to Microsoft

Eliminate **ALL** Admin accounts and move end users to standard access

But what happens to client satisfaction?

We Need Balance

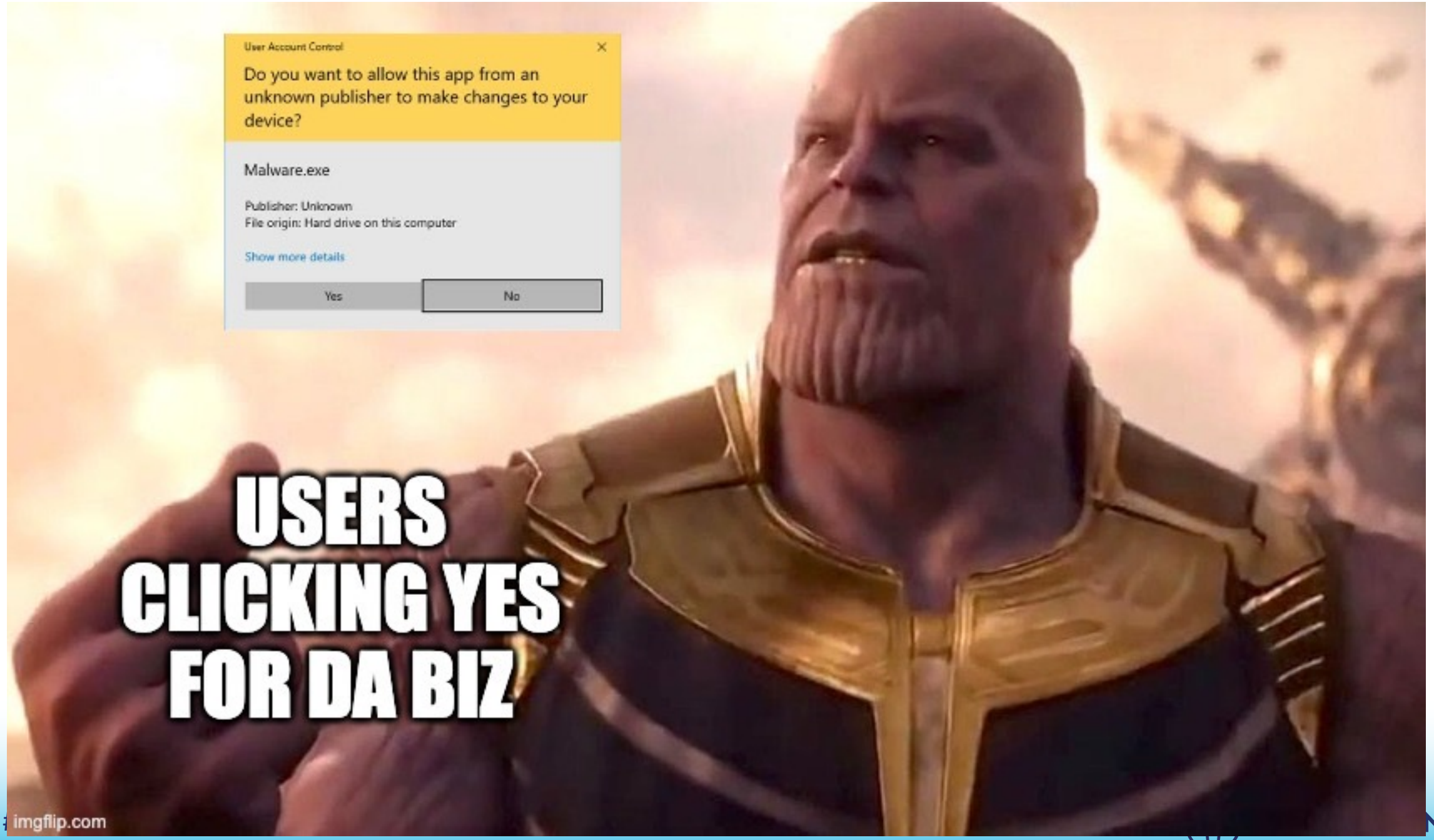
To Much Access



To Much Restriction


What’s the Default State?

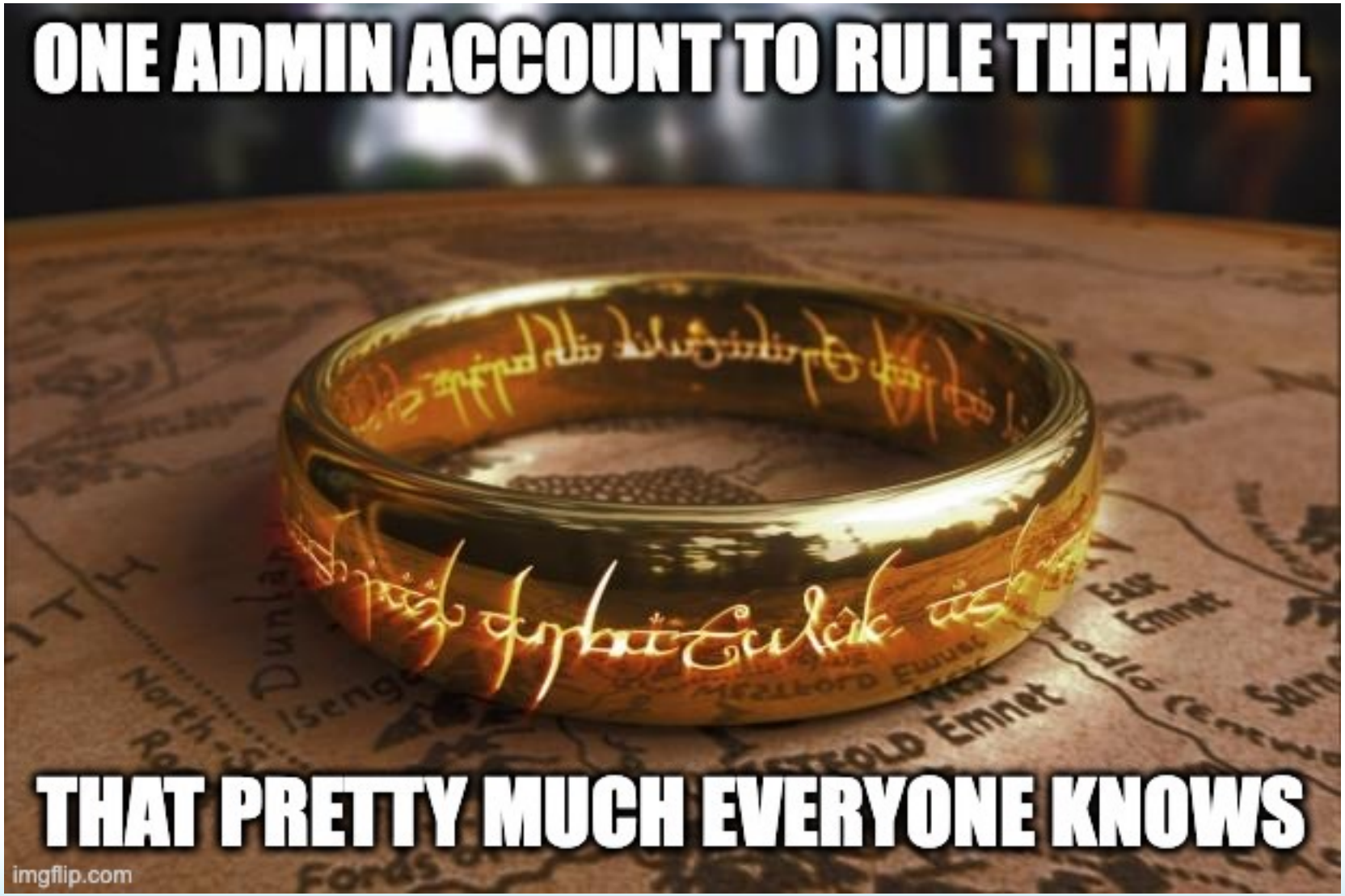

You need admin permission to do that.
Are you threatening me Master Windows?
The admin will decide your fate.
I AM the admin!


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your device?
Malware.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show more details
Yes
No
USERS CLICKING YES FOR DA BIZ
imgflip.com

What's the Default State?

- Line of business applications require local admin to operate or update, which makes life even worse
- The sprawl of this pain over the years tends to feel insurmountable.


YOU'RE AN ADMIN!
AND YOU'RE AN ADMIN!!!
EVERYONE GETS ADMIN!


ONE ADMIN ACCOUNT TO RULE THEM ALL
THAT PRETTY MUCH EVERYONE KNOWS
imgflip.com

"A unique admin account... for every tech... and every client"

So What Do We Do Next?

Trattoria al Forno
Allergy-Friendly Dinner Menu

PLEASE NOTE: Guests may consult with a chef or special diets trained Cast Member before placing an order. We use reasonable efforts in our sourcing, preparation and handling procedures to avoid the introduction of the named allergens into these menu choices. While we take steps to prevent cross-contact, we do not have separate allergy-friendly kitchens and are unable to guarantee that a menu item is completely free of allergens. Allergy-friendly offerings are reliant on supplier ingredient labels. We cannot guarantee the accuracy of the contents of each food item. Allergen advisory statements (e.g., "may contain") are not regulated and therefore ***not taken into consideration*** *when developing allergy-friendly meals. It is ultimately our Guests' discretion to make an informed choice based upon their individual dietary needs.*

Appetizers

Calamari Fritti Crispy Pepperoncini, Balsamic Agrodolce, Meyer Lemon Aïoli 17
For Gluten/Wheat, Peanut/Tree Nut, and Soy Allergies

Insalata Caprese Fresh Mozzarella, Tomatoes, Balsamic 13
For Gluten/Wheat, Egg, Fish/Shellfish, Peanut/Tree Nut, and Soy Allergies

Insalata di Stagione Seasonal Salad, House Ricotta, Vinaigrette 12

So, here’s how to message this…


UNION
SETTLEMENT

Privileged Access Management

Thank you!

Follow me at:

- CyberFOX.com
- Empathcyber.com
- Linkedin.com/in/wesspencer
- Youtube.com/wesspencer

IT Nation Secure

EXCLUSIVE: Any purchase of AutoElevate will get 50% off Password Boss!

IT NATION™ SECURE

Don't forget to fill out your

SESSION SURVEY