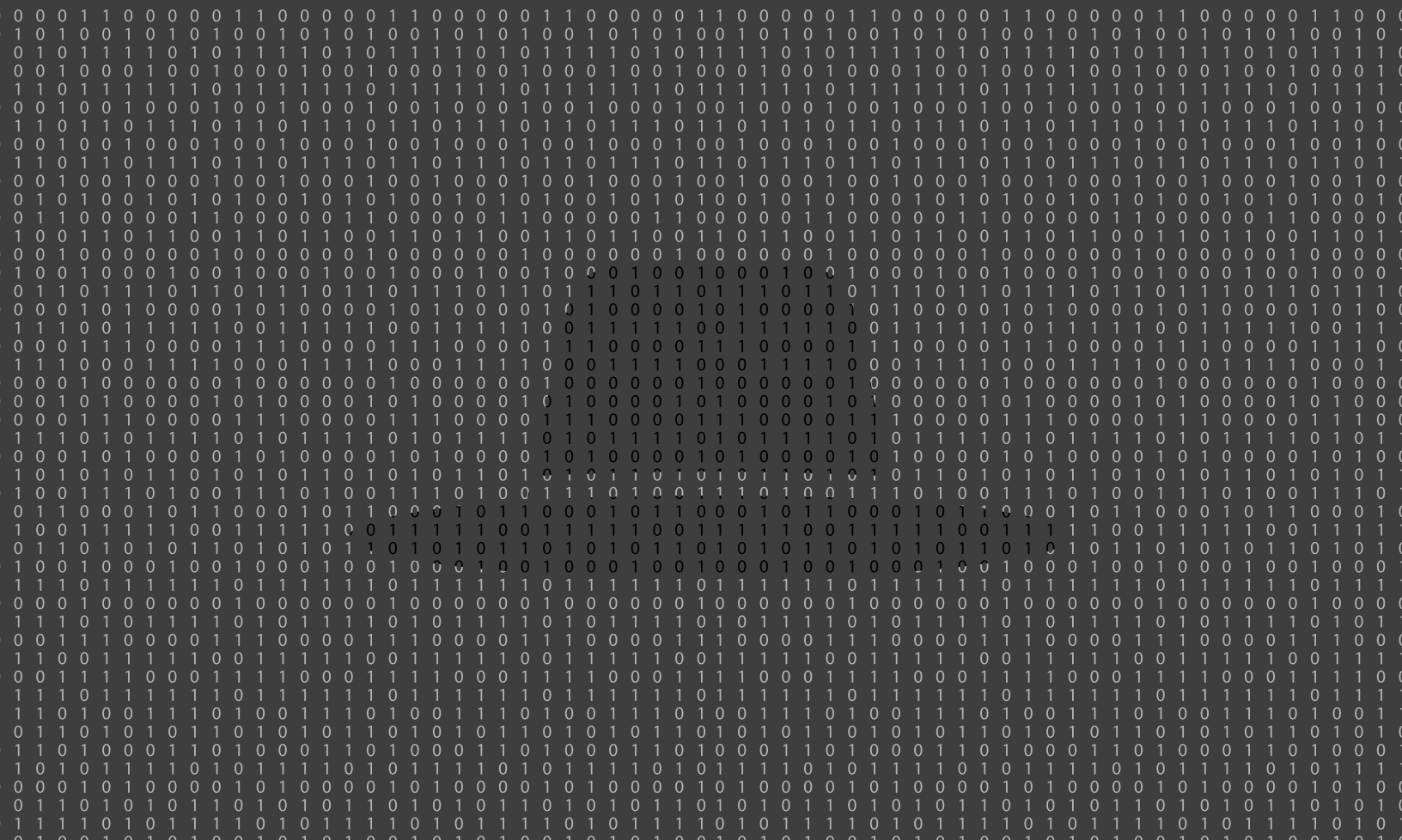
Black Hat 2016:

Hacker Survey Report



thycotic

Black Hat 2016: Hacker Survey Report

Hackers support data privacy but half are willing to crack your passwords for a price

Thycotic's most recent survey of hacker attendees at the Black Hat Conference, August 3 to 4 in Las Vegas shows overwhelming support for data privacy among respondents yet in a seeming contradiction of their own beliefs, half said they would be willing to hack your password for a fee if asked by the FBI. This in the context of a recent controversy when the FBI hired a third-party to help crack the password for the iPhone of a shooting suspect after Apple refused to help on grounds of protecting privacy.

Bottom line: more than 75% of Black Hat survey respondents believe no password is safe from hackers or the government for that matter. Here are some of the shocking highlights from the survey with a more detailed description of the findings on the following pages.

THE GOOD NEWS:
100% support data protection, security, and privacy.

Nearly all hackers supported data privacy and security and 4 out of 5 agreed with Apple that it should not have helped the FBI requests to crack the iPhone of the San Bernardino shooter. When the FBI was able to break into the iPhone by paying a third-party to help, one third of hackers think cybercriminals will be able to use the same methods for malicious purposes.

THE BAD NEWS:
Hacking for hire still a major threat if the price is right.

While recognizing the right to security and privacy, two thirds would be willing to hack into the iPhone for the FBI. Of those respondents willing to hack for hire, 73% would expect a payment ranging from $500,000 to more than $100 million.

THE SHOCKING NEWS:
9% would hack your password just for fun.

Even with support for data privacy, a shocking 9 percent of respondents said they would hack the phone just for fun...with no monetary compensation at all.

The bottom line: 77% say no password is safe from hackers—or the government

thycotic
PRIVILEGED ACCOUNT MANAGEMENT
p: +1 202-802-9399
e: sales@thycotic.com
www.thycotic.com

Black Hat 2016: Hacker Survey Report

Nearly one-third or 30% of Hackers believe that the government decrypting our data will cause more harm than good, and 40% of hackers believe if the FBI can do it (as in the Apple iPhone case), anyone can get access. In addition, 42% of Hackers believe that the government has been hacking and spying on our personal data for years, only now is this practice getting noticed. The result, 77% don't believe any password is safe from hackers.

Hackers share their secrets on how you can make their job more difficult

Privileged Passwords remain a primary target for hackers and most believe that no password is safe from cracking. Survey respondents however did offer advice to businesses that want to protect themselves from hackers, suggesting they start by implementing these key security measures:

1. Limit Admin access to systems
2. Protect Privileged Account passwords
3. Conduct more IT security awareness training and education
4. Limit unknown applications from running on the network
5. Protect user passwords with security best practices

p: +1 202-802-9399
e: sales@thycotic.com
www.thycotic.com

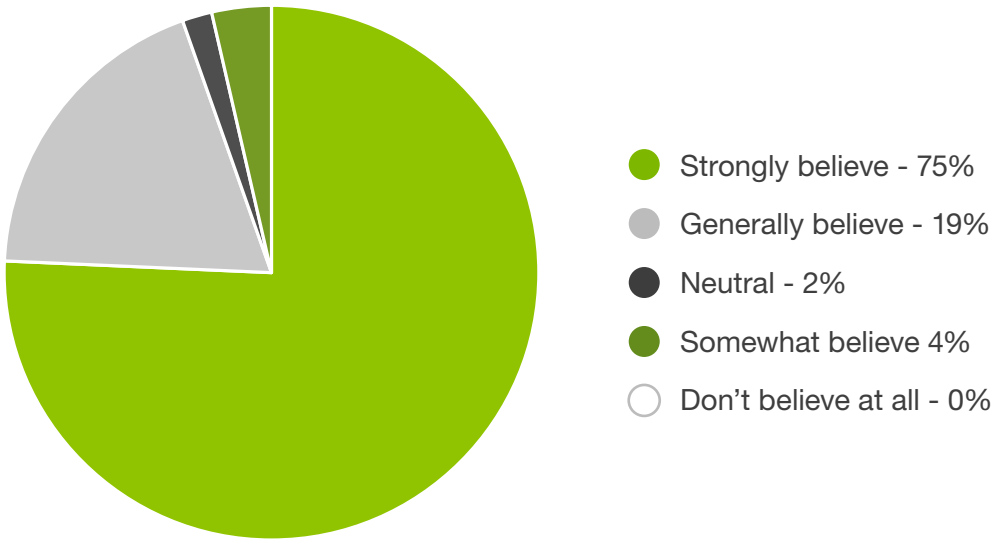
Black Hat 2016: Hacker Survey Report

Thycotic Black Hat 2016 Hacker Survey Executive Report

In an effort to learn more about the methods by which hackers are able to successfully break into and compromise enterprise networks, Thycotic sponsored a third annual official poll conducted live onsite at Black Hat USA 2016. Thycotic secured 250+ responses from Black Hat attendees, asking them to self-identify as white hat and black hat hackers, and the results documented herein reveal their attitudes toward data security and privacy along with their willingness to exploit weaknesses in password protection – in some cases just for fun and in others for a significant amount of money.

Not surprisingly, the survey respondents in general were not fans of the government's efforts to monitor the personal information of individuals using computer devices on the internet. They were split in their opinions of how the FBI's high profile success in hacking the password of the San Bernardino shooter's iPhone will affect the security of information going forward. The following pages describe in more detail the results of the survey.

? Do you believe that people generally deserve data protection, security, and privacy?

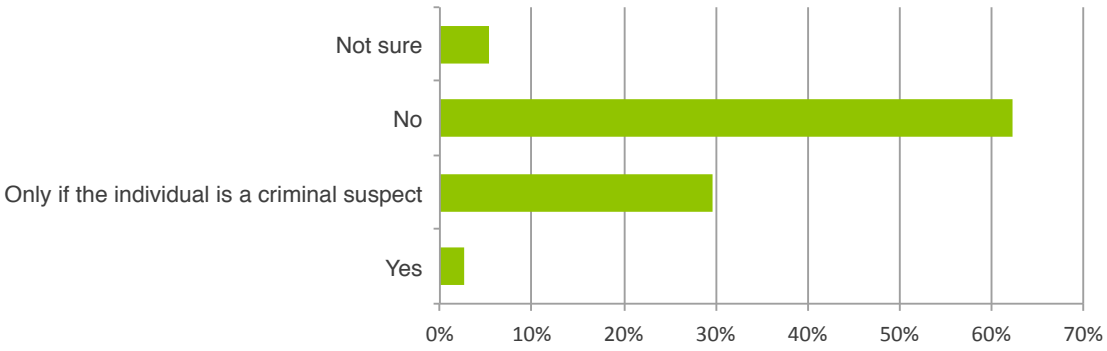


In general, the hacker survey shows overwhelming support for the premise that every citizen has a right to data protection, security, and privacy of their personal information.

p: +1 202-802-9399
e: sales@thycotic.com
www.thycotic.com

Black Hat 2016: Hacker Survey Report

Should any government be permitted to remotely access your home devices to monitor you without permission?

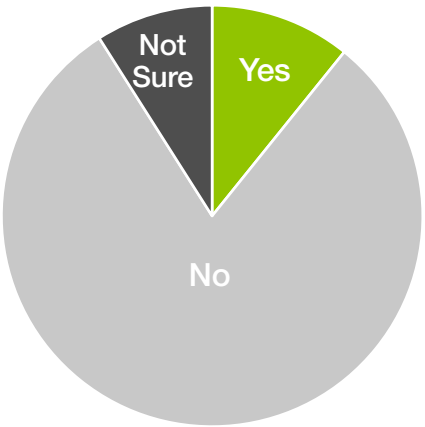


In addition, two-thirds do not feel the government has a right to access and monitor home computer devices without permission.

Yet this support for individual privacy is tempered by a belief that no password is safe from hackers, especially given the recent controversy surrounding the efforts by the FBI to obtain the password of an iPhone used by the shooter in the San Bernardino attack in December of 2015.

Should Apple have complied with requests to help the FBI crack into the encrypted information stored on the San Bernardino shooter's iPhone?

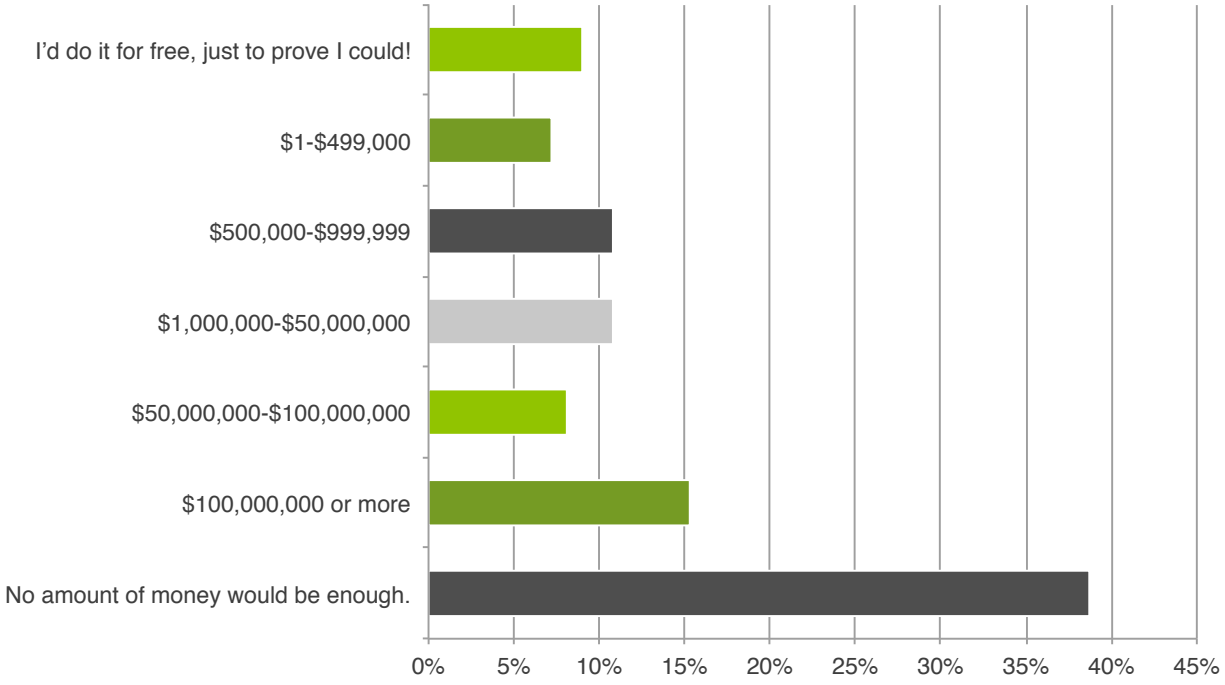
Four out of five survey respondents agreed that Apple was right in not complying with government requests to hack the shooter's iPhone. The FBI eventually paid $1.3 million to a third-party to crack the password, the largest ever publicized fee for a hacking job according to media reports.



thycotic
PRIVILEGED ACCOUNT MANAGEMENT
p: +1 202-802-9399
e: sales@thycotic.com
www.thycotic.com

Black Hat 2016: Hacker Survey Report

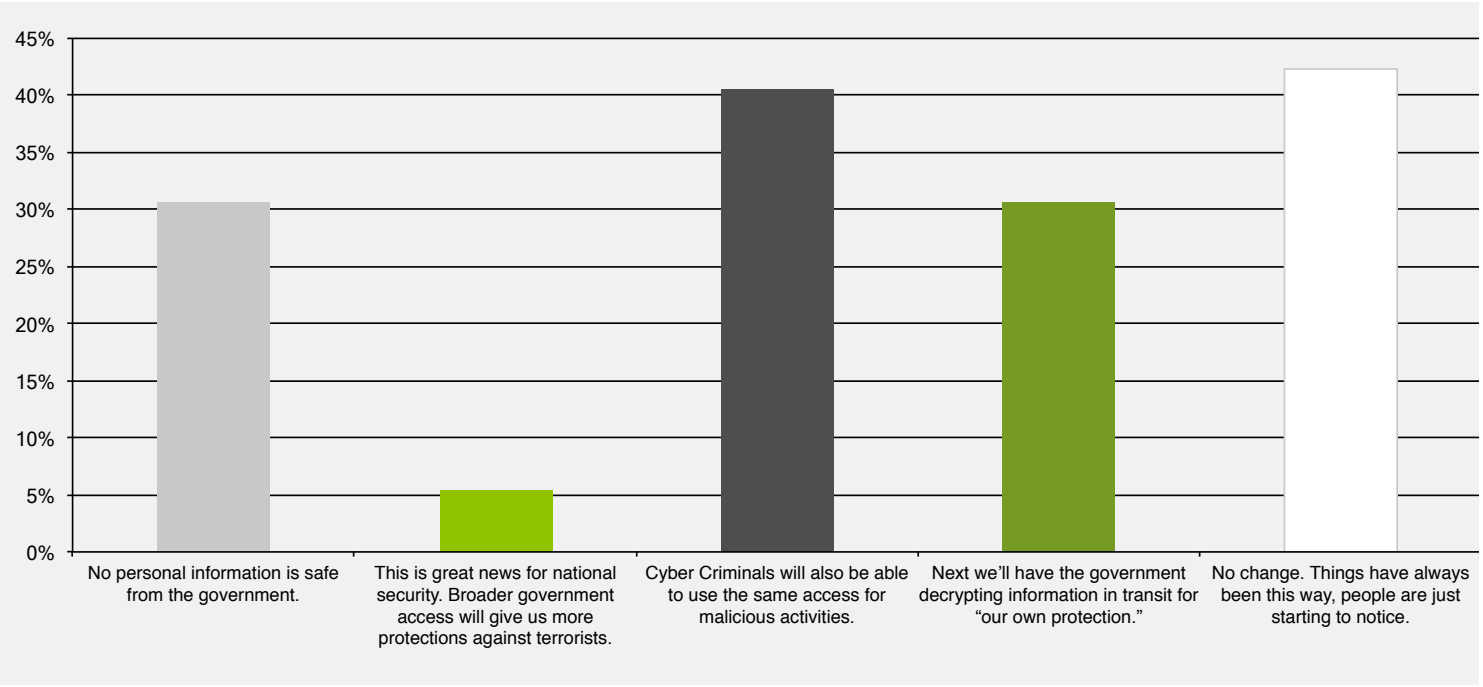
If asked by the FBI to help crack into the iPhone, how much would you demand to be paid?



However, in seeming contradiction, a substantial set of respondents—52%—said they would be willing to help the FBI crack the iPhone password for money. And among those who would be willing to hack the password for a fee, 18% would do it for under $1 million, 10% said they would do it for $1 million to $50 million, and another 23% would be willing to crack the password for a payment of $50 million to $100 million or more. Over one third of respondents said that there was no amount of money that would induce them to help the FBI hack the iPhone.

Black Hat 2016: Hacker Survey Report

Now that the FBI successfully paid a third party to crack into the encrypted info stored on the iPhone – where will it lead? (Pick as many as apply)



The successful hack of the iPhone by the FBI, has several implications for the hackers in the survey. Nearly one-third or 30% of Hackers believe that the government decrypting our data will cause more harm than good, and 40% of hackers believe if the FBI can do it (as in the Apple iPhone case), anyone can get access. In addition, 42% of Hackers believe that the government has been hacking and spying on our personal data for years, only now is this practice getting noticed.

Bottom line, 77% don't believe any password is safe from hackers.

thycotic
PRIVILEGED ACCOUNT MANAGEMENT
p: +1 202-802-9399
e: sales@thycotic.com
www.thycotic.com

Black Hat 2016: Hacker Survey Report

Hackers share their secrets on how you can make their job more difficult

Privileged Passwords remain a primary target for hackers and most believe that no password is safe from cracking. Survey respondents however did offer advice to businesses that want to protect themselves from hackers, suggesting they start by implementing these key security measures:

1. Limit Admin access to systems
2. Protect Privileged Account passwords
3. Conduct more IT security awareness training and education
4. Limit unknown applications from running on the network
5. Protect user passwords with security best practices

1 Limit Admin access to systems

Privileged Accounts are the top target of any attacker to gain access and move anywhere within a network. First, attackers gain a foothold in the network by any means possible, often through exploiting an end-user computer, then working to elevate their privileges by compromising a privileged account, which allows attackers to operate on a network as if they are a trusted IT administrator.

Adopting a least privilege strategy, where privileges are only granted when required and approved, eliminates the chances for an attacker to compromise your network by targeting privileged account passwords or hashes. Enforce least privilege on end user workstations by keeping end users configured to a Standard User profile and automatically elevating their privilege to run only approved and trusted applications. For IT Admin privileged accounts, control access to the accounts and implement Super User Privilege Management for Windows and UNIX systems to prevent attackers from running malicious applications, remote access tools and commands. Get Started with Windows Application Control and Privilege Manager for UNIX.

2 Protect Privileged Account Passwords

With the increasing complexity of IT infrastructures, it's not uncommon to have two to three times more privileged accounts than employees. Thus, hijacking privileged accounts gives attackers the ability to access and download an organization's most sensitive data, poison data, broadly distribute malware, bypass existing security controls, and erase audit trails to hide their activity. It is critical to proactively manage, monitor, and control privileged account access – these accounts are necessary to today's IT infrastructure and ensuring they are securely managed is critical.

p: +1 202-802-9399
e: sales@thycotic.com
www.thycotic.com

Black Hat 2016: Hacker Survey Report

All too often organizations still rely on manual systems such as spreadsheets to manage their privileged account passwords. This is not only inefficient, but such systems are easily hacked posing a major security risk to the entire enterprise. Privileged Account password protection provides a comprehensive solution to automatically discover and store privileged accounts, schedule password rotation, audit, analyze and manage individual privileged session activity, and monitor password accounts to quickly detect and respond to malicious activity. This adds a new layer of security to protect privileged accounts from inside the network. Get Started with Thycotic Secret Server.

3 Extend IT Security Awareness Training

The weakest link in most organization's security is the human being. As more sophisticated social engineering and phishing attacks have emerged in the past few years, companies need to seriously consider expanding their IT security awareness programs beyond simple online tests or acknowledgements of policies. Especially as personal mobile devices are increasingly used for business purposes, educating employees on secure behaviors has become imperative.

4 Limit Unknown Applications

Application accounts need to be inventoried and undergo strict policy enforcement for password strength, account access, and password rotation. Centralized control and reporting on these accounts is essential to protect critical information assets. Thycotic least privilege and application control solutions enable seamless elevation of approved, trusted and whitelisted applications while minimizing the risk of running unauthorized applications. Get started with Application/Service Account discovery through Secret Server and Application Control.

5 Protect User Passwords with Security Best Practices

While privileged accounts are the most coveted credentials to provide attackers with critical data access, end-user passwords are also a major attack vector for hackers. Enforcing strong password policies on end-user credentials helps protect these identities from being compromised during an attack.

Passwords for end-users should be reset, at a minimum, every 30-90 days, and be complex. Password changes should be audited and performed via a self-service password reset mechanism to ensure your security policy's password complexity requirements are enforced, provide an audit log for compliance, and improve employee experience by greatly reducing help desk calls, empowering end-users to take control of their own password resets, and increasing ROI for internal support costs. Get Started with Password Reset Server.

p: +1 202-802-9399
e: sales@thycotic.com
www.thycotic.com

Black Hat 2016: Hacker Survey Report

Next Steps

Given that privileged accounts are prime targets for hackers, IT professionals would be wise to consider the recommendations of the hackers themselves when it comes to protecting privileged account access. Thycotic provides innovative free tools and automated PAM security products that deliver simple, easy to use and affordable solutions to protect your privileged accounts and improve the security of your IT infrastructure. You can learn more by visiting www.thycotic.com and reviewing the free tools listed here.

Free Privileged Account Discovery Tool for Windows

Find out how many of your Windows Privileged Accounts are at risk.
https://thycotic.com/solutions/free-windows-privileged-account-discovery-tool/

Free Privileged Account Password Vulnerability Benchmark

Benchmark your organization against others in your industry to see how your security practices rank.
https://thycotic.com/solutions/free-password-vulnerability-benchmark-tool/

Survey Methodology

In August 2016, Thycotic surveyed 250+ attendees including self-identified hackers live at the Black Hat 2016 conference in Las Vegas. "Hackers" were defined as official attendees of the Black Hat conference who personally identified themselves as a hacker at the time of the poll. Respondents remained anonymous to protect their personal identity. For more information, please email sales@thycotic.com.

p: +1 202-802-9399
e: sales@thycotic.com
www.thycotic.com