thycotic

RSA SURVEY REPORT

Employee Social Network Password Practices a Major Workplace Risk

EMPLOYEE SOCIAL NETWORK PASSWORD PRACTICES A MAJOR WORKPLACE RISK

53% say they have not changed social network passwords in more than a year!

A survey conducted by Thycotic at the RSA Conference in San Francisco in February, 2107, revealed some startling and disturbing insights into password practices by participants representing cybersecurity professionals from across the globe.

One of the most striking results from the survey was the lack of common sense password security practices around social media usage---and its potentially devastating consequences for employers if/when employee social media accounts are hacked or compromised.

THE PROBLEM

More than half of survey respondents at RSA (53 percent of users) haven't changed their social network passwords in more than one year – with 20 percent having never changed their social media passwords at all.

80% of all cyber security attacks involve a weak or stolen password.

THE RISKS

With nearly half respondents at the RSA conference not changing social network passwords for at least a year, hackers can often exploit social network accounts and infiltrate users' other accounts including work computers and email.

Once compromised, a social network account can easily allow hackers to access information that will grant them access to other facets of users' lives, such as their work computers and email. And, when a hacker takes over a Facebook or Twitter account, the hacker can readily social engineer attacks on the victim's co-workers, colleagues, friends, and relatives.

THE CHALLENGE

Large social networks don't remind or make clear to users the risks associated with using weak passwords, or never changing their passwords. In fact, new social network platforms allow for a single logon that is linked to multiple social media accounts so that users can avoid having to remember multiple passwords for multiple accounts.

PASSWORD PRACTICES REMAIN A MAJOR VULNERABILITY---EVEN AMONG CYBERSECURITY PROFESSIONALS

The RSA survey results also revealed a major disconnect between security professionals and their own cybersecurity habits. This may be due in part to what researchers are calling "security fatigue," whereby users feel overwhelmed with security warnings and revert to habits they are most comfortable with, but which may put their organizations at greater risk of a breach.

THE PROBLEM

Nearly 30 percent of security professionals have in the past, or still use, birthdays, addresses, pet names or children names for their work passwords---all readily hackable.

THE RISKS

User accounts in the workplace are still highly vulnerable, even those used by security professionals who should know better. The fact that the people who are on the front lines of ensuring day-to-day security for businesses are using weak passwords for their credentials should raise an alarm among all organizations.

50% **of respondents haven't changed social network passwords for a year or more.**

THE CHALLENGE

Security professionals must devote more attention to implementing best practices for password management among themselves, along with implementing automated tools that will help all users to fight "security fatigue" and safeguard user and privileged accounts.

KEY FINDINGS AND RECOMMENDATIONS

Here are several key findings from the RSA Conference survey along with corresponding recommendations based on password security best practices and resources available to IT administrative and security professionals.

20% of respondents have never changed their social network passwords ---ever!

RECOMMENDATION:

Protect all user passwords with 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---especially for social media accounts. Enforcing strong password policies on end-user credentials helps protect these identities from being compromised during an attack.

Most social media users, for example, do not use multi-factor authentication for logging into social media sites, and many people still use weak or reused passwords—putting their accounts at risk of being hacked. Because many people use Facebook or Twitter authentication and passwords for multiple sites, a takeover of one's Facebook or Twitter account can, in fact, mean the compromise of many other accounts as well---including those in the workplace.

30% of security professionals have used or still use birthdays, addresses, pet names or children names for their work passwords---all readily hackable.

RECOMMENDATION:

Expand and refine 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, as well as social networking, educating employees on secure behaviors has become imperative.

25% of respondents said they change their password at work only when the system tells them to.

RECOMMENDATION:

Safeguard user passwords with best practice enforcement

Passwords for end-users should be changed, at a minimum, every 90-180 days, and be easy to remember but complex for example using a passphrase or password vault. 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.

45% of respondents believe at least half of the cyberattacks against their companies involved privileged passwords.

RECOMMENDATION:

Protect Privileged Account passwords with automated tools

With Forrester estimating up to 80% of breaches involving privileged accounts, security pros appear to significantly underestimate the risks from privileged password threats and abuse. And it seems to reinforce that old habits of relying on manual systems such as spreadsheets to manage their privileged account passwords are not only inefficient, but such systems can be easily hacked, posing a major security risk to the entire enterprise. Software solutions such as Thycotic Secret Server, provide Privileged Account password protection that automatically discovers and stores privileged accounts, schedules password rotation, audits, analyzes and manages individual privileged session activity, and monitors password accounts to quickly detect and respond to malicious activity.

LEARN MORE ABOUT HOW YOU CAN IMPROVE PASSWORD SECURITY

While privileged accounts are the most coveted credentials targeted by attackers to gain critical data access, end-user passwords are also a major attack vector for hackers. Properly storing and managing privileged account credentials as well as enforcing strong password policies on end-user credentials helps protect them from being compromised.

Thycotic provides free password security educational resources and software tools to help you protect your user and privileged accounts at www.thycotic.com/free-tools .

FREE PASSWORD SECURITY LEARNING TOOLS

- **Free Privileged Password Security Online Training** ensures you and your staff are up-to-speed on the importance of privileged account security and best practices to protect passwords.

- **Free Security Policy Template for Privileged Passwords** saves hours of time and effort with easy-to-customize templates that help you improve security and meet compliance mandates.

FREE PASSWORD SECURITY SOFTWARE TOOLS

- **Free Weak Password Finder for Windows Tool** gives you an immediate and easy way to Identify where the weak passwords are located across your organization.

- **Free Privileged Account Discovery for Windows Tool** enables you to find privileged accounts across your enterprise, including many that are unknown and unmanaged.

- **Free Windows Endpoint Application Discovery Tool** saves you hours of effort by discovering vulnerable applications and their associated risks in minutes.

FREE PASSWORD SECURITY BENCHMARKING TOOLS

- **Free Password Vulnerability Benchmark** lets you see how your password protection efforts compare with those of your peers.

- **Free Security Measurement Index** online survey shows you how your IT security effectiveness compares with best practices and those of your colleagues.

ABOUT THYCOTIC

Thycotic prevents cyberattacks by securing passwords, protecting endpoints and controlling application access. Thycotic is one of the world's fastest growing IT security companies because we provide customers with the freedom to choose cloud or on premise software solutions that are the easiest to implement and use in the industry. Thycotic has grown to serve more than 7,500 customers.