FASTPASSCORP

WHITEPAPER

The ultimate solution to protect your service desk against social engineering

Learn what typically creates service desk breaches - and how you can fix it

Table of Contents

Introduction

Your service desk can issue users new passwords when they forget theirs. This is a necessary and beneficial service, but problems arise when hackers impersonate users to steal their passwords.

Since the widespread implementation of IT passwords, a “forgotten password” has presented a formidable challenge for users and service desk supporters. Initially, service desks would issue a new password as soon as possible to get the user back to work. This was, however, before the explosion of IT crimes and data breaches.

Hackers need passwords to perform a successful data breach – according to Verizon DBIR, more than 80% of data breaches include a stolen or weak password. Manipulating service desk supporters to get the desired information through social engineering methods can have devastating consequences for your company.

As one of the best-known white-hat hackers, Kevin Mitnick has stated in his book The Art of Deception, ***“Why should an attacker spend hours trying to break in when he can do it instead with a simple phone call?”***

This white paper delivers crucial information about security risks at the service desk, and a secure and comprehensive solution to safeguard your organization against social engineering attacks.

CHAPTER 1

Real life service desk attacks

The attacks on service desks are not a theoretical issue. They have affected numerous organizations, and some have openly published the details.

In this chapter, we'll go over some recent attacks on well-known businesses, so you can become aware of the pitfalls and how to keep your company's data secure.

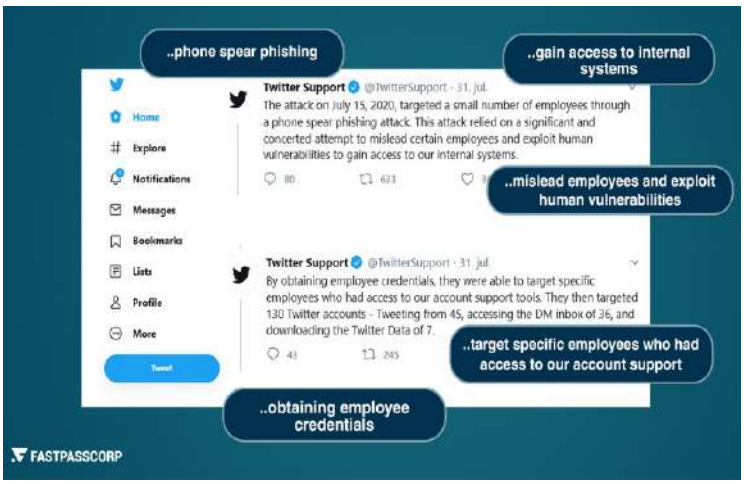
The highest-profile case was the **Twitter attack** in July 2020, where a young hacker accessed celebrities' Twitter accounts by obtaining privileged passwords from the Twitter service desk.

Twitter

The Twitter support team openly explained what happened. The simple explanation is:

A hacker exploited human vulnerability when calling up a specific Twitter group (the internal service desk) to obtain the credentials (password) to gain access to internal systems.

In this case, Twitter only lost credibility and trust. Hackers can cause much more severe harm once they gain access to a system.

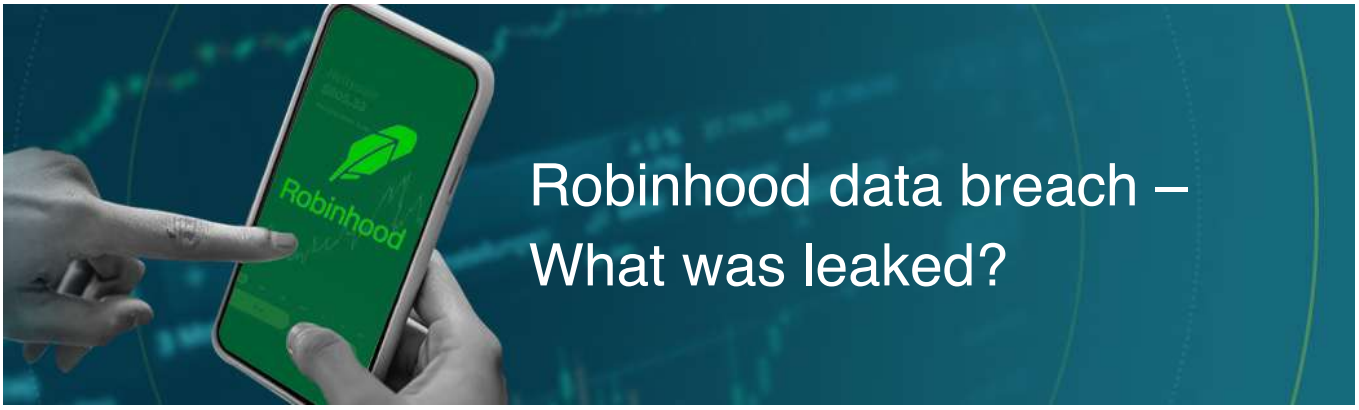


This illustration outlines how the hacker got into Twitter's system by targeting a small group at the service desk. In a social engineering attack, even a seemingly minor security gap can potentially result in catastrophic consequences. Fortunately for Twitter, there was no great financial loss – but once inside a system, a hacker can get a blank check to your company's assets. If this hacker used his expertise on your service desk, would your organization be safe?

Once an internal system is hacked, there's no limit to the damage that can ensue – does your business have the security required to prevent the next "Twitter attack"?

Robinhood

Robinhood, which had already been facing controversy in 2021, announced in November that it had suffered a security breach. The breach dates back to November 3rd, when it said that an "unauthorized third party obtained access to a limited amount of personal information for a portion of our customers."



In a blog post, Robinhood stated that the unauthorized party "socially engineered a customer support employee by phone and obtained access to certain customer support systems." The data affected by this breach included email addresses for around five million people, and the full names of approximately two million members in a separate group. In this case, the breach involved the leaking of confidential information and the Twitter attack resulted in reputational damage.

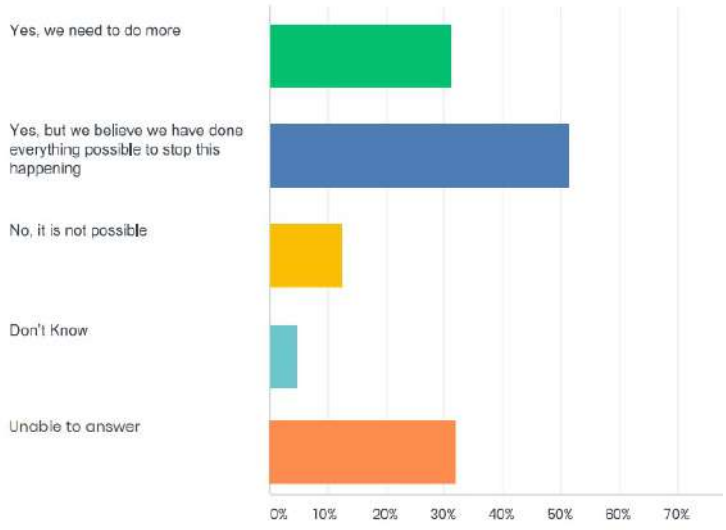
Besides losing sensitive data and trustworthiness, other serious outcomes of a data breach include revenue loss, operational downtime, theft of intellectual property, and legal action.

What are service desk managers saying?

A survey asked Service Desk Institute (SDI) members the following question:

“Despite your authentication process, do you think it is possible for a criminal (internal or external) to get a password for a legitimate end-user’s account?”

As can be seen from the graph on the following page, the answers were astonishing:



Of the active respondents, **83% agreed that there is a risk that a password can be obtained from their service desk!** As illustrated in the chart, more than 50% realize the security risk, but don’t think there is any option to avoid it.

FastPass IVM addresses this risk, significantly increasing the security at the service desk. It is a solution that these survey respondents were not aware of, and one of great interest for the IT service desk manager who wants to safeguard an organization against rampant social engineering attacks.

Consequences of a Data Breach

Hackers have different objectives with their attacks. In a worst-case scenario, an attack could even force a business to shut down.

The world’s largest container-line, Maersk, was another data breach victim. This attack was not directly related to the service desk but had a disastrous outcome. According to Maersk, the operational loss exceeded US$300 million!

The main takeaway here is not how the hackers managed to destroy the Maersk IT infrastructure, but the consequences that such an attack can have. A significant user’s stolen password is one very critical piece in the puzzle that hackers make.

Questions for reflection

1. Has your service desk seen attempts to get credentials from unauthorized users?

2. Do you have solid processes to report and register such incidents?

CHAPTER 2

The focus and job of your service desk

Earlier, we referred to them as a “Help Desk.” It aptly described their duty to help users with problems – and in the IT world, this means IT problems.

With more and more organizational processes supported by IT workflow, the productivity of an entire organization relies on the users’ ability to use IT efficiently. Any problems with users or the IT system always needed a quick resolution, or else the company’s productivity would decrease. It followed naturally, therefore, that the first commandment for the service desk was: “Help the users – see them as your customers!”

For management, however, it presented itself as a cost center. Since organizations must keep costs at a minimum to remain competitive and efficient, service desk management introduced tight measurements and KPIs to reduce the service desk’s total costs. As a result, it outsourced many service desks to managed service providers and low-salary countries.

Still, around 20-30% of all “tickets” in the service desk are related to password calls. In critical environments like these, security is paramount, and a wrong decision can jeopardize the organization’s security.

Training the service desk

The supporter at the service desk is the key to the final quality. We also understand from many service desk managers that there is a high turnover of supporters, and it is challenging to keep them trained and up-to-date on all the tasks within various systems when users call in.

As a substitute for training, clear instructions can suffice. However, this method only works if the particular instructions are available when the supporter needs them! Within a dynamic service desk environment, the only way to ensure a reliable system is to build the instructions into the ITSM solution.

The demands of today and the future

With the explosion of data breaches and IT attacks, no IT department can afford to ignore IT security. End-user service levels and cost per transaction can no longer be the only KPIs for IT management.

The service desk must implement reliable security and a “no trust” philosophy.

The biggest problem for security is the human-to-human interaction, as emotions are involved and are prone to persuasion. The competent hacker knows this and will try to play on the supporter’s emotions to steer them away from following their instructions.

The future of service desk will continue to demand:

- **User service level**
- **Low cost per transaction**

It must, however, be without security risks. Service desks must implement security measures and processes wherever gaps present potential security risks.

How do you handle password resets today?

Efficient processes for protecting the password reset process often include:

- **Company questions**
- **Personal questions**
- **Use of tokens like SMS**

When in “solution mode,” it is essential to remember the particular challenges that can arise when dealing with password problems. For example, if the user is not logged in, even routine transactions like sending an email or connecting to a workstation are not accessible.

Questions for reflection

1. What is your current verification process for users calling in?

2. What is your current procedure for compliance reports and alerts for password resets?

3. Can supporters circumvent your verification process/ instruction?

4. Are all password reset calls logged in your ITSM system?

CHAPTER 3

What does it take to safeguard the service desk against social engineering?

Hackers primarily use two very different social engineering techniques to obtain a password from the service desk. They are likely to:

- **Know the answers to the questions or tests presented**
- **Manipulate the supporters' emotions to make them give the desired information**

Preparing the answers

A skillful hacker will typically call the service desk numerous times, asking for different users' passwords. He will note the questions and use social media to research the correct answers. You might argue that this can take a long time. That's undoubtedly true, but if the hacker can earn a million dollars in an attack, he can invest considerable time in the preparation.

If it is an internal job, it becomes even easier for the criminal to obtain the necessary information to answer the tests correctly.

The use of tokens strengthens the security of password questions and answers. One of the most common tokens is an SMS code sent to the user's mobile phone, which works well in preventing simple hacks. It proves unreliable when more advanced hackers can spoof the mobile number and get a copy or the original SMS code. The US NIST (National Institute of Security and Technology) warns against using SMS codes for higher-level security use.

We must understand that hackers learn these techniques as part of their profession. In turn, we must be professional to win the battle. For example, we must include elements in the security checks that the hackers cannot prepare for. We call these elements dynamic and contextual data. A hacker cannot anticipate answers that change dynamically. Where are you (geo-location) – is this reasonable? Are you working from home? If so, do you have your home PC available then?

The primary emotions the hacker will play on

Instead of trying to answer the questions, some hackers use manipulatory techniques to get the supporter to deviate from the standard question and answer procedure.

You might think that a technical hacker is not likely to have these skills. Maybe not, but a simple Google search will lead you to educational material on how to develop the manipulative skills of social engineering. These classes are intended for 'white-hat hackers' to do customer penetration tests. So, how do we prevent 'black-hat hackers' from gaining competence?

Why service desk employees give passwords to hackers

In an ideal scenario, no service desk supporter will give a password away to the wrong person. If a caller sounds suspicious, hopefully the supporter would interrupt the call or take appropriate action. Unfortunately, an adept hacker doesn't seem suspicious!

The real world for the supporter might entail a heavy Monday morning workload with a long line of waiting callers. The aim is to give satisfactory and efficient service to all of them. In the line, a single hacker waits. The odds are like a match between a professional tennis player against an ordinary amateur. The amateur will lose at least 99 out of 100 times.

Eliminating emotions from the verification process

The best way to protect the supporter and IT security is to transfer the management of the process from the supporter to an intelligent workflow. When the workflow manages the supporter, the hacker can no longer use emotions against the workflow; it is machine logic which runs the process!

When a hacker finds out that nothing will change, no matter how much charm or intimidation, they will most likely try their techniques on the next company!

CHAPTER 4

A customer case using FastPass IVM

One of our customers experienced attempts to attack the service desk and implemented the FastPass Identity Verification Manager to protect the corporate passwords against vishing (Voice Phishing) attacks on the service desk.

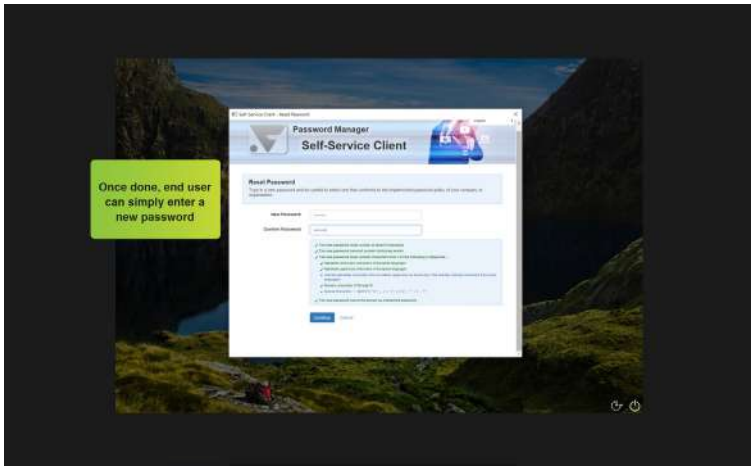
When the supporter receives a password-related call, the system automatically transfers it to the IVM workflow. A specific workflow is initiated based on the user-ID's relationship within the group.

A typical work-flow proceeds like this:

- **IVM asks the supporter to instruct the user to click on the password icon on the user's workstation. If it is a workstation that the user often uses, the supporter will get a green light and continue.**
- **The user answers a question about their phone number and continues if correct.**
- **IVM prompts them to give the number from the OKTA TOTP app.**
- **The user answers a question about their manager.**

If the user answers all questions correctly, the password application on the user's PC opens, and they can enter a new password twice. Of course, it follows the company's password policy.

The process is fast, as all data is present for IVM, and the supporter doesn't need to open different systems.



There are simpler verification processes for lower-profile groups in less critical contexts.

The customer blocks the supporters' access to the Windows password-reset function as part of the implementation. This prevents the hacker from getting the supporter to circumvent IVM.

All data is registered and available for compliance reporting and use for SOCs.

Questions for reflection

1. What will you include in a secure verification process?

2. Do you have other corporate passwords than Active Directory? Like SAP, Oracle, IBM, etc.

3. Who is responsible for password security in your organization?

4. Do you have a password protection plan that covers all processes?

FASTPASSCORP

CHAPTER 5

Identity Verification certified by ServiceNow

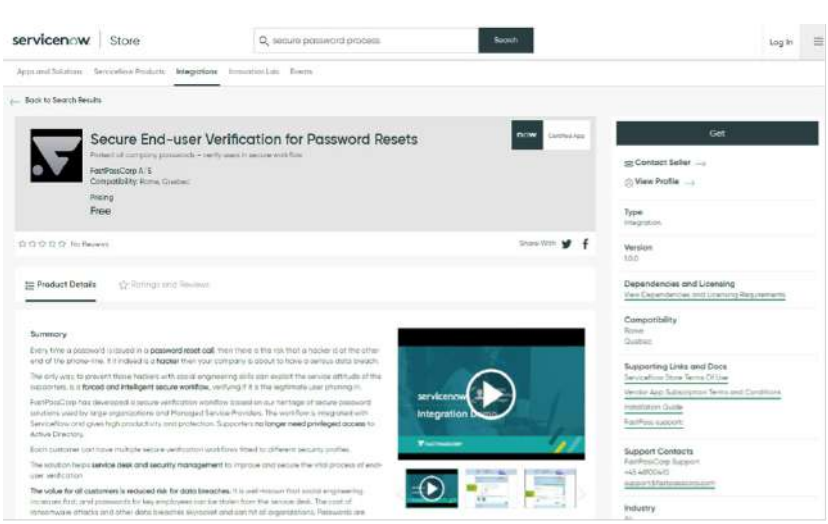
FastPassCorp has been in the software business for more than ten years, developing secure password solutions for large organizations and managed service providers.

With the launch of IVM, we met a strong demand to make a complete integration to the customers' ITSM-systems. As IVM is completely integrated with service desk operations, we have designed IVM to integrate with all modern ITSM systems seamlessly.

The IVM for ServiceNow

Considering the proliferation of ServiceNow implementations at large organizations, we decided to make the first complete integration for ServiceNow.

The integration between IVM and ServiceNow is now certified by ServiceNow and is available from the ServiceNow Store.



At the ServiceNow Store, you can see a three minute demo of the supporter's workflow in an interaction with a user. You can connect directly to FastPassCorp for technical details and more information.

The integration is between the ServiceNow cloud and the FastPassCloud. This means that you can very easily test the integration and the security of the workflow when using the ServiceNow integration.

If you prefer to have FastPass installed on-premise, the integration will work for this too, and the user functionality is identical to the cloud version.

Pricing

The FastPassCloud solution is priced according to user count. The monthly cost per user is approximately as much as a cup of coffee!

With 5,000 users, the monthly cost is US$3500 for Windows passwords. The price for an on-premise solution is lower than this.

Get a Free Demo

At FastPassCorp, we've addressed the need for heightened service desk security and have designed our range of solutions to seamlessly integrate with your IT infrastructure. Now that you've become familiar with the security risks and potentially drastic consequences, the next step is to take a closer look at the solution to protect your data from social engineering attacks.

Some of the next steps you can take:

Find more information at the ServiceNow Store

Find more information at the FastPass website

Request the guide to secure identity verification process from FastPassCorp

Book a meeting to discuss your situation and requirements

Book a free trial for IVM-ServiceNow - FastPass Cloud

Get a price quote from FastPassCorp

How can you find out more:

Book a free online demo meeting

Discuss your organization's specific requirements

Determine an individual quotation

FINN JENSEN
CEO I FASTPASSCORP

Technology changes at a rapid pace, and we have developed a solution to protect your service desk against social engineering attacks – a solution that has been a decade in the making.

We invite you to a free demo meeting online to discuss password security for your particular situation.