intercede

Prevent Identity Theft with Two-Way Identification

WHITE PAPER

Executive Summary

Establishing mutual trust when contacting customers over the phone has benefits for both parties. Traditionally, an organization needs to verify that they are speaking to an account holder, but due to increased social engineering scams, customers are more and more wary of providing security information over the phone, leading to an impasse and long call times.

A viable solution should have shared knowledge and a standards-based way to generate a one-time code for verifying that the other party is in possession of the secret, without divulging this directly to any unwanted third parties. A satisfactory solution should also be simple to use and implement.

Pattern-based authentication, provides an excellent way to address the two-way identification problem and is included as part of the core product. Implementing a two-way identification system reduces identity theft, lowering the risk of litigation resulting from data breaches, improves customer retention, and reduces call centre costs.

1. Introduction

Your customer receives a phone call from a person claiming to be from your company with an urgent account issue. The person on the phone tells them they need answers to some security questions before they proceed.

How is your customer meant to know if this is a legitimate phone call or another social engineering scam? Most of the time it is almost impossible to tell the difference before it is too late.

A two-way identification process is required to give both the caller and recipient of the call certainty of each other's valid identity. Here we discuss the problem and outline a cost-effective solution.

2. Social Engineering Vector

Sometimes it is the simplest attacks that cause the most damage. We are all too familiar with the attacker who uses their technical savvy to infiltrate protected computer systems to compromise sensitive data. This type of hacker is in the news all the time. This, in turn, motivates those responsible for the protection of sensitive data to invest in new technologies to further improve network defences.

However, there is another kind of attacker who uses different tactics to circumvent our tools and solutions. They are the social engineers who specialize in exploiting the one weakness found in every organization: human psychology. Using phone calls and social media, these attackers trick people into offering them access to sensitive information.

While identity theft and fraud have been around for a long time, attacks of this type have steadily increased, as has the media interest associated with them. With growing reliance on IT systems, the protection of user data housed within IT systems has become critical. Recently introduced legislation, such as EU General Data Protect Regulation (GDPR), means that the penalties could be severe should any type of customer data be compromised. To conform with data protection legislation, and to protect business interests, corporations must take steps to ensure that a client's identity is verified during all phone calls or online communication.

3. The Identification Dilemma

Your bank or utility provider phones you to discuss a problem with your account. To comply with data privacy legislation, companies must prove that you are who you say you are. Before even knowing what the call is about, you must first endure a battery of 'security' questions to confirm your identity.

We have all experienced that scenario. Frequently, the questions asked, and answers provided, were established when the account was opened. They follow a similar pattern, such as "state your mother's maiden name", "what is the city of your birth", and so on. Alarmingly, most of these questions can be answered by studying an individual's social media pages. Whilst this type of authentication is simple to enable and is simple for customers to understand and remember, using it may not be the best approach, especially when pertaining to the security of valuable information.

We are conditioned to expect a pattern of answering security questions when contacted by banks and utilities. This expectation exposes a client to a surprisingly simple and dangerous attack. While answering questions correctly may well prove the client's identity to the bank, how does the customer know that the person phoning is indeed from the bank? Or if they work in an open plan office, do they feel comfortable answering these questions with others in earshot?

Equally alarming is the fact that even if the caller works for the bank, they now have access to all your details. How do you know they won't pass these onto someone who can use those 'secure' details to impersonate you in future? Sadly, syndicates that work in banks and outsourced call centres are a reality we can't ignore either.

4. Establishing Mutual Trust

To solve this problem, we need to find a mechanism that allows both parties to verify that they are who they say they are. This must be done in a way that does not allow a simple replay of information by a bad actor at a later date.

A solution should also be easy to implement and place low barriers to entry for the customer. Since customers are more concerned with the level of service and call time than security, any solution should be straightforward for customers to use.

Both parties should have access to a common piece of information, or secret. Crucially, this information itself should not be divulged on the call. Rather, it is used to generate a onetime code that can be divulged by either party which confirms that they are in possession of the secret. Verifying that the person you are speaking to is in possession of the secret, confirms that they are the person or organization with whom you initially shared this value.

Since the secret is never divulged after the initial setup, it is also reasonable to assume that no third party has had access to this information. Since the codes are single use only, a third party cannot subsequently use the code to impersonate anyone at a later stage.

Standards such as the one set by the Initiative for Open Authentication (OATH) already exist to generate one-time code from a shared secret value. This collaborative effort of IT industry leaders aims to provide a reference architecture for universally strong authentication across all users and devices separated over networks. OATH tokens such as Google Authenticator are already commonly used to provide an additional layer of security when logging into sensitive computer systems. It turns out that this mechanism can be also be used to solve the two-way identification problem, and uniquely, in a way that does not require a separate mobile device or plastic token.

5. Pattern Based Authentication as a Solution

Pattern Authentication allows users to generate one-time codes from a pattern on a grid of numbers. Pattern Authentication is based on research findings into how people remember information. People are far better at remembering shapes and patterns than arbitrary text, such as a password. The pattern itself remains known only to the user, and because the numbers on the grid change every minute (generated by an OATH-compliant algorithm), it is an ideal candidate to generate one-time codes for two-way identification.

A big advantage that Pattern Authentication has over other OATH-based systems is that a grid can simply be printed on a bank statement or utility bill. A customer does not need to have an app installed on a mobile phone or plastic token available to provide their one-time code, although an app-based solution is also available to incrementally improve security from a 1.5 factor to 2 factor level of authentication.

The representative of the organization making or receiving the call can verify their identity to the user by providing a portion of the grid for a specific statement, or for that point in time, without having access to the full grid. At the same time, the user can then authenticate themselves to the bank or utility by providing the one-time code generated from the pattern in their head which is then verified on the other end of the call.

A banking customer called Bob receives a call from a bank agent called Jane. To continue the call, the bank, Jane, must verify herself to the customer, Bob. Bob must also verify himself to Jane, establishing mutual trust. When Bob receives a phone call from the bank he checks his latest bank statement for a printed pattern authentication grid or checks his bank supplied application on his smartphone which can display a grid to Bob.

On her system, Jane can see only the top line of the PINgrid challenge grid visible to Bob within his pattern authentication application. Jane reads out these numbers to Bob who, looking at the application, can verify these numbers. If they match, Bob will know for certain that Jane is indeed an agent calling from his bank.Now that Bob trusts Jane, Jane can ask Bob for his pattern authentication one-time code which he then supplies, using the pattern stored only in his head to generate a one-time code that Bob gives to Jane. Jane enters this code into her system. Once the system accepts this code as being correct, Jane can be sure that Bob is indeed Bob.

By using pattern authentication for the two-way identification process, two key features have been accomplished. Firstly, Jane and Bob can be certain that the other is who they say - ensuring data protection legislation, corporate policy, and security best practices have all been satisfied. Secondly, none of the information exchanged thus far is of a sensitive nature which might be used maliciously in the future. This process stops fraud resulting from identity theft in its tracks.

A further benefit emerges from this. Because the identification process is well understood by both parties and is simple and transparent, the identification part of the call can be over in seconds. Because a significant amount of time per call is traditionally spent on identification– over 50% in some cases –

6. Advantages of Pattern Based Authentication

Introducing pattern-based authentication comes with a range of obvious benefits- improved security for both users and businesses being the number one, but let's explore some of the other advantages:

Patterns Are Not Divulged

When users enter a password, this password is divulged to the system so that it can confirm the password is correct. This leaves a footprint of the password and opens up room for potential breaches. Unlike passwords, patterns are not transmitted between the user and the server, meaning that hackers cannot access the pattern.

Shoulder Surfing Risk is Reduced

When someone is spying over a user's shoulder, they are looking out for the numbers or letters of the password, rather than the pattern. With pattern-based authentication, learning the code means nothing for the thief, as the code will change from minute to minute - only the pattern remains the same.

Avoid the effort and expense of Multi-Factor

Pattern-based authentication can be used with efficacy in isolation to allow users to login with a one-time code, without the need for a second physical device. This makes for a quick and low-cost deployment and is a drop-in replacement for a password login.

Step up to Multi-Factor when needed

Where stronger authentication is required, the user can enrol a device as a second factor - a mobile phone or tablet, for example. This adds an additional layer of security, as the challenge grid is physically separate to the logon. The user would have to have control of the device and know the pattern to logon. This step up in security is seamless to the user as the logon experience is the same.

Easy Integration

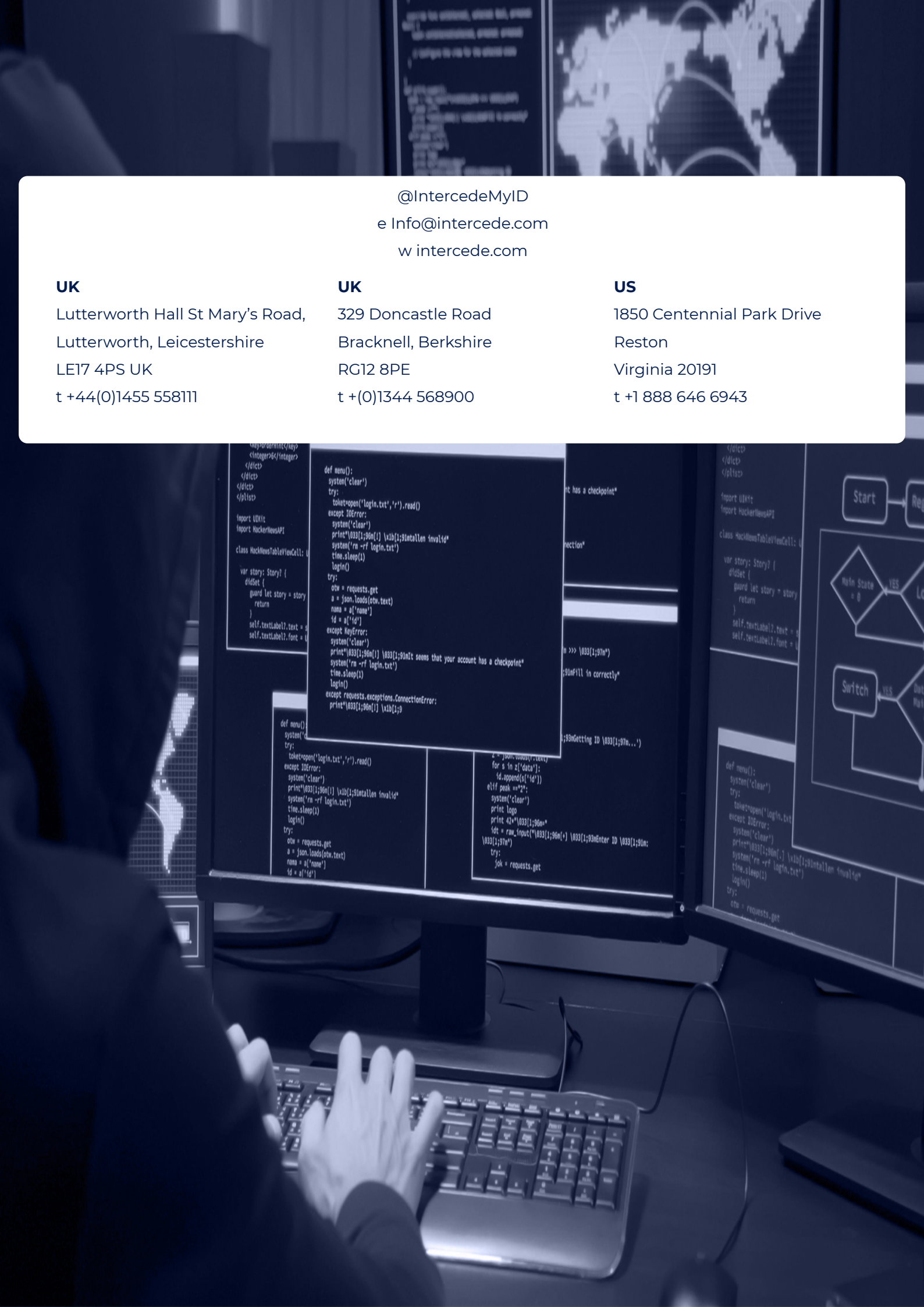
Pattern-based authentication can be easily integrated into networks and applications via standards-based methods such as SAML and RADIUS, which require no developer interaction.

7. Conclusions

Social engineering often bypasses even the best security systems by exploiting human nature. An effective strategy must include information only known to relevant parties and this information should not be divulged as part of the establishment of mutual trust.

Solutions exist that could easily be implemented, using existing mechanisms such as printed statements, or mobile phone applications and these applications should leverage an existing standard such as OATH, rather than implement a custom security pattern which is almost always flawed.

Benefits from implementing a two-way identification solution include an increase in security, lowering exposure to litigation from a data breach, prevention of loss of customer loyalty and trust from complicated processes or perceived weak security, and direct financial benefit from reduced call times.



@IntercedeMyID

e Info@intercede.com

w intercede.com

UK

Lutterworth Hall St Mary's Road,

Lutterworth, Leicestershire

LE17 4PS UK

t +44(0)1455 558111

UK

329 Doncastle Road

Bracknell, Berkshire

RG12 8PE

t +(0)1344 568900

US

1850 Centennial Park Drive

Reston

Virginia 20191

t +1 888 646 6943