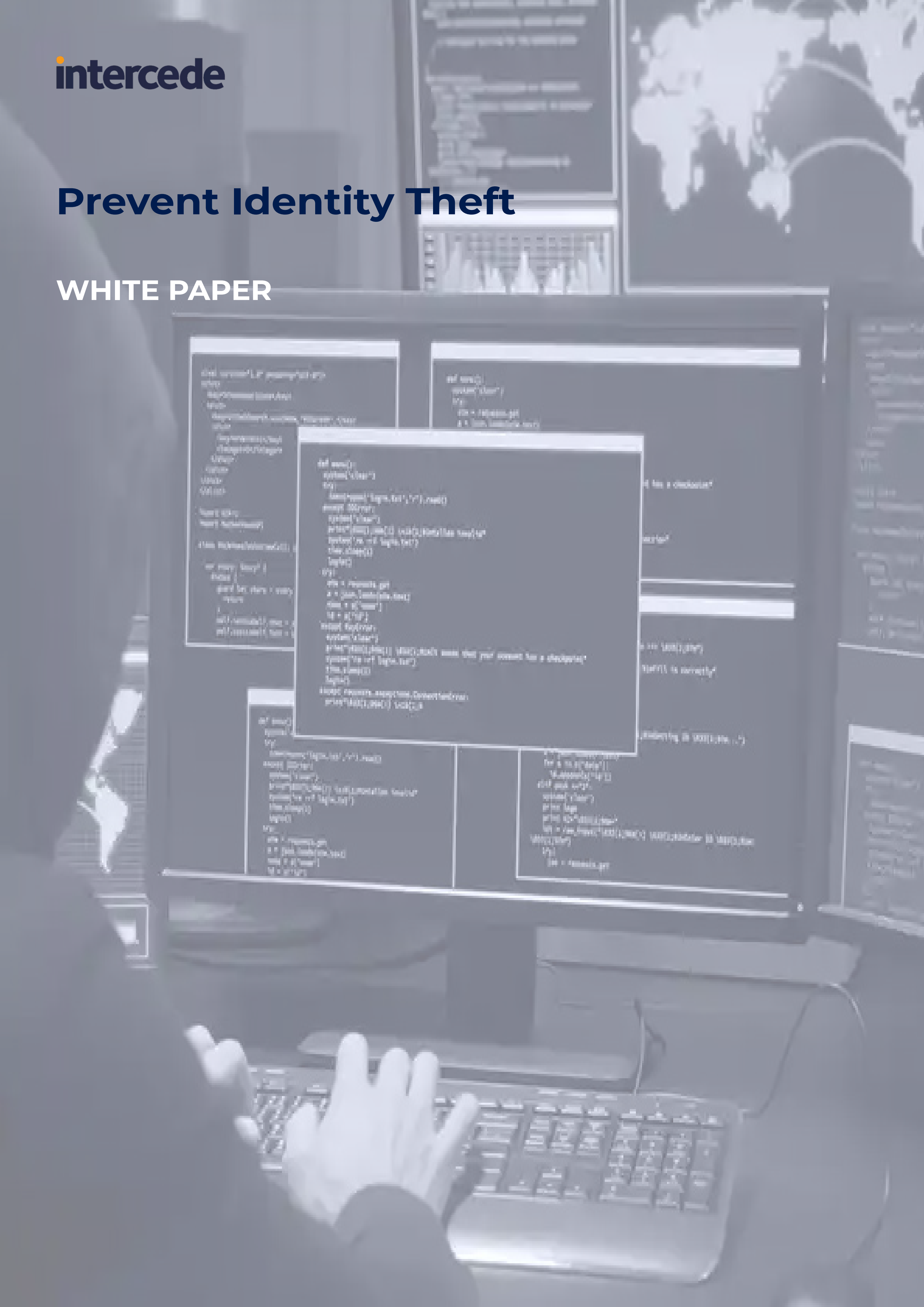
intercede

Prevent Identity Theft

WHITE PAPER



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

Social engineers specialise 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.

3. The Identification Dilemma

To comply with data privacy legislation, companies must prove that you are who you say you are, however, in order to do this, you must endure various 'security' questions.

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.

While you are proving your identity to the bank, how do you know that the person phoning is indeed from the bank?

Equally alarming is the fact that even if the caller works for the bank, how do you know they won't pass these onto someone who can use those 'secure' details to impersonate you in future?

4. Establishing Mutual Trust

In order to establish mutual trust, you need to find a mechanism that allows both parties to verify that they are who they say they are. A solution should also be easy to implement and place low barriers to entry for the customer.

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 one-time code that can be divulged by either party which confirms that they are in possession of the secret. 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. OATH tokens such as Google Authenticator are already commonly used to provide an additional layer of security when logging into sensitive computer systems. This mechanism can 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

The Cybersecurity Maturity Model Certification (CMMC) is a certification and compliance process developed by the Department of Defense (DoD). Released in January 2020, CMMC brings together a collection of compliance processes namely NIST SP 800-171, NIST SP 800- 53, ISO 27001, ISO 27032, and AIA NAS9933 to certify that contractors have the controls in place to protect sensitive data.

CMMC requires DoD contractors to have their systems audited by a 3rdparty now. The contractor remains responsible for the implementation, monitoring, and certification of the appropriate cybersecurity controls.

Pattern Authentication is a patented and award-winning technology that allows users to generate one-time codes from a pattern on a grid of numbers. Pattern Authentication is based on research that found people are far better at remembering shapes and patterns than arbitrary text, such as a password.

6. 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