# EFFECTIVE ID PROTECTION: GOOD PASSWORD HYGIENE + BREACH DETECTION

ID protection solutions offer service providers new ways to reach target audiences. Service providers should carefully choose a solution that not only swiftly detects a breach, but prevents it from happening in the first place.

F-Secure

# CONTENTS

# INTRODUCTION

The identity protection market, already an established business in North America, is currently emerging in Europe as a new security category. And with new reports indicating the current global health crisis is only exacerbating identity theft and other online crime, consumers may be needing effective identity protection solutions more than ever.

According to a recent study by Finanso.se, identity fraud, already widespread across European countries, has become the second most common type of fraud in Europe. Javelin Research predicted account takeover fraud and scams will only increase in 2020 given the global health and financial crisis, as criminals are more active during periods of economic adversity. EU Commissioner Ylva Johansson recently warned of growing identity theft and other online fraud as people spend more time at home.

The problem is already a very real consumer concern, according to 2019 research from F-Secure. 56% of consumers are worried about their personal information leaking in a data breach; 55% are concerned about online shopping fraud; and 58% are worried about their bank account being hacked.

The data also shows consumers are worried enough to consider a solution: 52% say that an alert system when private or sensitive data has been exposed is an attractive product benefit. 26% are willing to pay for such a service, and 34% would like to purchase it through their mobile or broadband operator.

# THE STAGE IS SET

The timing has never been more opportune, it seems, for service providers considering getting in on the emerging trend of identity protection solutions. IDP solutions can help service providers create fresh new marketing angles and reach new target audiences. The solutions appeal to the "sweet spot" of Generation X, as exemplified by the 46% of identity theft victims in the UK who were between the ages of 30 and 49.

But before service providers jump to offer this intriguing new product area, it bears considering the way these products work, as not all IDP offerings are equal. Service providers should take care to choose a solution that provides their consumers the right balance of effective ID theft detection and abuse prevention.

The current identity protection offerings on the market in both consumer and service provider domains typically offer reactive monitoring for exposed consumer data, and alerts when such data is found so victims can take action to mitigate the damage. But to offer consumers the most comprehensive, effective ID protection solution, an offering should also include proactive measures that put consumers in a better position to prevent the crime from happening.

When considering which offering to take into use, it helps to have an understanding of how ID theft happens and how the online crime world works.

# HOW ID THEFT HAPPENS

When we think of identity theft, we often think of the worst-case scenarios – a social security number being stolen and a mortgage being taken out in the victim's name, or bank accounts being drained. While these cases are devastating, the vast majority of today's ID theft actually happens as account takeover, which, according to Javelin, saw 72% growth in 2019.

Losing access to one's Netflix account because it's been hacked is one example of account takeover. And while it sounds less menacing, this form of identity theft can quickly spread from, for example, a Netflix account across an individual's other online accounts. With each account, the perpetrator gains greater access to the victim's sensitive details and online life, and more opportunity to do financial or other damage.

How does account takeover spread across accounts? Ironically, the answer lies in the very thing that is supposed to protect our accounts from unauthorized access: Passwords. But because most of us have so many online accounts, it's beyond our ability to easily remember a unique and strong password for each account. Too many people re-use the same password across accounts, effectively giving anyone who cracks that password the "keys to the kingdom."

In itself, this might not be such a dangerous habit if not for the fact that criminals are constantly using various methods of stealing login credentials, from employing malware and phishing campaigns to stealing user data from breached online services. In the case of data breaches, once criminals steal data, they share it online with other criminals. They use automated tools to crack encrypted passwords. Because shorter, weaker passwords are faster and easier to crack, criminals focus on those.

Once a set of passwords is decrypted, the attackers can begin breaking into accounts with automated password spraying tools – tools that let them attempt the cracked passwords against large numbers of online accounts to find combinations that work. Once they find a password that works against a victim at one service, they can use that password to compromise various other services associated with that victim.

# PROACTIVE PROTECTION MEANS PASSWORD MANAGEMENT

If we go back to the idea of an ID monitoring service, there's no question that such a service is helpful. But because of humans' tendency to use and reuse weak passwords, ID monitoring alone stops short of addressing the source of the problem.

What can get to root of the issue is password management. Password managers help users generate a strong, unique password for each and every online account. The good ones make this so simple that logging in with a password manager is even easier than re-using a weak password.

This is why F-Secure, the leader in partnering with service providers to offer value-added security solutions, includes as part of its ID protection solution a powerful, easy to use password manager. F-Secure ID Protection incorporates the functionalities of the popular consumer app F-Secure KEY, bringing the benefits of password management to service provider customers.

The result: A unique ID theft protection solution that focuses on lowering the risk of ever falling victim to ID theft and account takeover in the first place. With integrated password management, F-Secure ID Protection offers something truly unique on the market.

"Password managers help users generate a strong, unique password for each and every online account."

Of course, there's no 100% security and although risk can be greatly reduced, it can never be zero. So what if a user is doing all the right things, employing a password manager for unique, strong passwords, and their data is still compromised?

That's when, as the saying goes, time is of the essence.

# THE NEED FOR SPEED

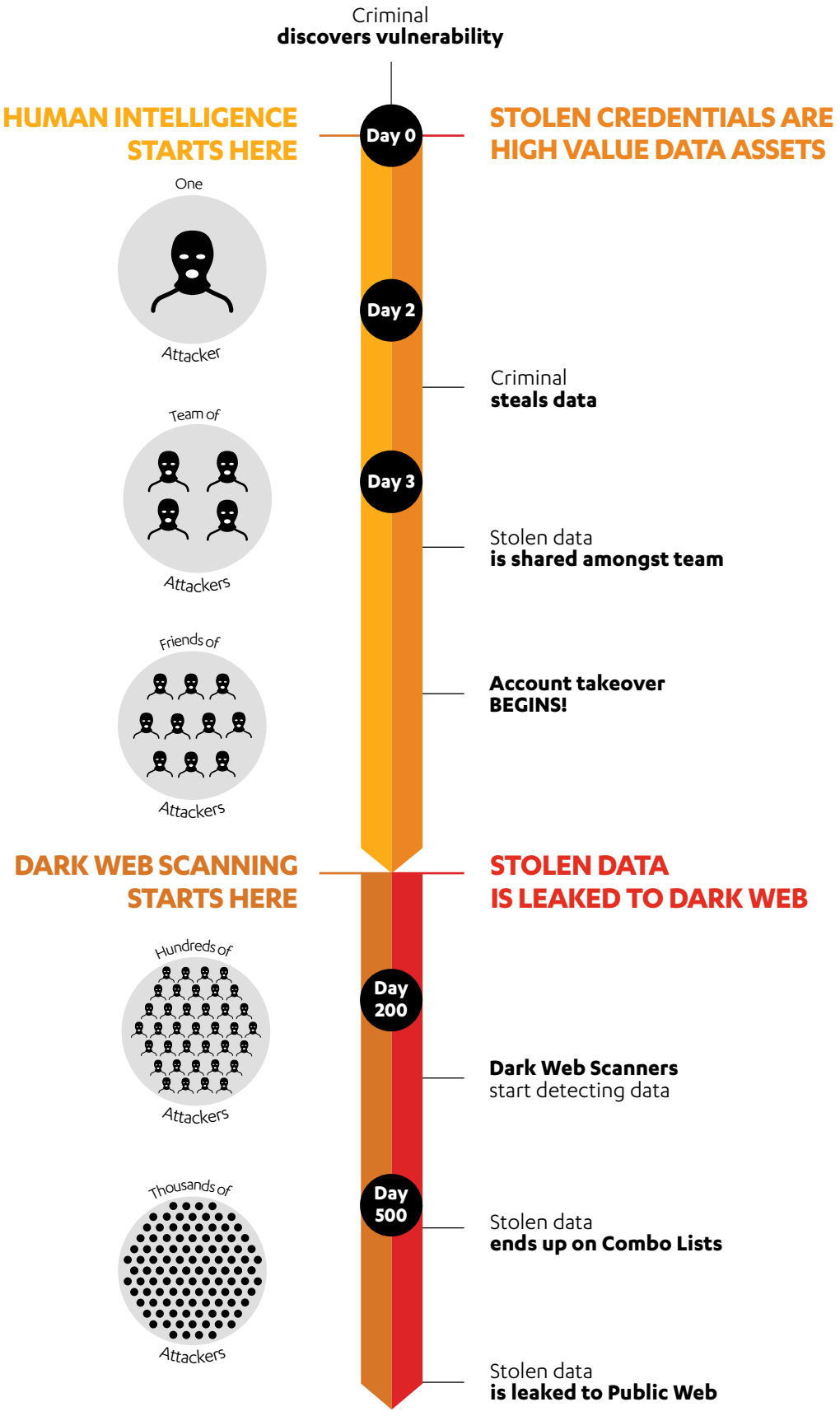
When attackers breach a service and exfiltrate password data, it typically only takes a few days for them to decrypt the passwords. Once the data is decrypted and ready for use in password spraying attacks, attackers can start taking over accounts.

Eventually, breached data makes its way to the dark web, the part of the internet that is inaccessible to search engines and where online criminals buy, sell, trade and dump stolen data.

Decryption is often done with the help of an attacker's close colleagues. They communicate to one another via what's known as the underground web, the deepest part of the web where "black hat" hackers and bad actors directly engage. This is where the data starts touching more hands. First circulated amongst a small group, as the data is passed around, it reaches a wider distribution among the attacker's friends and acquaintances.

Eventually, breached data makes its way to the dark web, the part of the internet that is inaccessible to search engines and where online criminals buy, sell, trade and dump stolen data. Here on the dark web, the data is available to hundreds or even thousands of potential attackers.

# THE BREACH TIMELINE




Effective ID protection: good password hygiene + breach detection

Most ID protection monitoring services work by monitoring the dark web and alerting their users when user data is found there. The trouble is, by this stage, the data has most likely already been abused and monetized. While it never hurts for victims to know their data has been compromised, at this stage, it may well be too late to prevent damages to their online profile or financial accounts.

This is why speed is so important – the earlier a victim's data can be found after a breach, the more well-positioned the victim is to stop abuse and exploitation of their online accounts and prevent identity theft. Discovering the problem before data even reaches the dark web allows the victim to take control before their data is exposed to entire markets of cyber criminals.

## HUMAN INTELLIGENCE

While other solutions don't detect stolen data until it reaches the dark web, F-Secure ID Protection has a unique ability to detect exposed data long before. On average, F-Secure ID Protection is able to detect stolen data 6 to 9 months earlier than others on the market, often within mere days of an initial breach.

That's not to say F-Secure's solution doesn't employ dark web monitoring, because it does. But the real reason F-Secure can identify breached data so quickly is because its solution also includes a human intelligence aspect provided by teams of skilled researchers. These experts have, over the years, credibly built up multiple personas on the underground web, that deepest part of the web where attackers directly communicate. There, the researchers use these personas to socially engineer attackers, leveraging the trust they have established to gain access to breached data in the earliest phases.

"On average, F-Secure ID Protection is able to detect stolen data 6 to 9 months earlier than others on the market, often within mere days of an initial breach. "

As attackers are naturally highly distrusting of every new contact, building up a network in the underground web is something only possible with years of dedicated effort. It's an effort that has paid off: F-Secure enjoys the best hit rates and discovery times on the market. "Hit rate" refers to the probability of finding and associating leaked data with a specific monitored email address. While competitors typically talk about 30% hit rates, F-Secure's hit rate is 55%.

# ATTRACTIVE LICENSING, NEW WAYS TO ENGAGE

Industry-best hit rates, fastest discovery times and the preventive capabilities of password management are the reasons service provider customers will be better protected. But in addition, F-Secure ID Protection also boasts an easy family licensing model with monitoring for multiple email addresses, so the whole household can enjoy ID Protection under one subscription.

The solution's app-based approach gives service providers a better way to engage with customers than email, as alerts, notifications and response guidance reach users wherever their device is. And with F-Secure, providers can have the opportunity to upsell customers on other products in the complete security portfolio, including Internet Security, Connected Home Security, VPN, Password Management and more.

ID protection offerings are now emerging on the EU market, making it a great time for service providers to launch their own version of a solution. With F-Secure, service providers get a high-ARPU service that's already perfected for the channel, with supporting processes, services and tools for the greatest possible success. But most of all, with human intelligence market-unique components, F-Secure ID Protection is the most effective form of protection to provide the best value for service provider customers when their data is compromised – and to prevent it from compromise in the first place.

# ABOUT F-SECURE

Nobody knows cyber security like F-Secure. For three decades, F-Secure has driven innovations in cyber security, defending tens of thousands of office, homes, and millions of people. F-Secure shields enterprises and consumers against everything from advanced cyber attacks and data breaches to widespread ransomware infections. F-Secure's AI-driven solutions also help to protect the connected devices and homes of your customers The unique combination of technology and world-class Business Services supporting the entire customer lifecycle is what makes F-Secure an excellent fit for the service provider channel. F-Secure's products are sold globally by more than 200 service providers and thousands of resellers.

**www.f-secure.com/identity-protection**

F-Secure