BEST PRACTICES:
NOTIFYING CUSTOMERS

Of Third-Party Breaches & Malware Exposures

SpyCloud

CONTENTS

THE PROBLEM

It's no longer a question of 'if,' but 'when' – your customers will reuse passwords across their multiple accounts, and those passwords will be exposed in a data breach or compromised as a result of a malware infection. As soon as compromised or reused passwords become available to cybercriminals, your customers are at high risk of account takeover fraud. With access to user accounts, cybercriminals can easily drain funds, siphon loyalty points, and make fraudulent purchases using stored credit card details. In cases where additional information is exfiltrated or exposed, bad actors can easily create new identities that leverage stolen PII and financial information.

Leaving your consumers vulnerable when they are at high-risk not only disrupts internal workflows and protocols, but also puts a strain on the organization – consumers today heavily rely on and expect the brands they transact with to protect their information and their digital identity.

SpyCloud enables you to protect your customers from cyber threats like account takeover, session hijacking and fraud, by proactively identifying credentials that have been exposed to cybercriminals in third-party data breaches or exfiltrated via a malware infection. By validating your users' identities and resetting compromised consumer passwords promptly, you can lock out potential attackers before they have a chance to use for additional cyber attacks, ensuring a secure digital experience for your users along every step of their journey with you, on a continuous basis.

Use this guide to craft messaging to your customers in the event their data is exposed in a third-party breach or malware infection.

PREVENT FRAUD, WITHOUT ADDING FRICTION

When you identify compromised credentials, the language you use to notify consumers that their passwords must be reset requires careful consideration. Informing affected users that their credentials have been exposed on the criminal underground can encourage them to choose strong, unique passwords and protect any other accounts that share the same login information. On the other hand, some consumers may wonder how you located their information on the 'dark web' in the first place and where it was exposed.

To prompt your consumers to take quick action without creating concern or friction, you'll need to craft effective communications that fit your brand and inspire confidence and trust. Based on input from SpyCloud customers, this playbook covers best practices for identifying your consumers' information in third-party breaches or as a result of a malware infection, notifying them that their credentials and other sensitive PII have been compromised, and getting them to take appropriate action to protect themselves and their accounts.

1 IDENTIFY AFFECTED CUSTOMERS

Your first order of business is to find out which customers are impacted.

- Identify and export list of affected accounts
- Choose your notification path:
  - A personal note from your internal support leader (best for smaller volume exposures)
  - Mass communication via your CRM or marketing automation platform (best for larger volume exposures)
- Partner with your marketing teams to craft the messaging of the notification (examples provided later in this guide)

2 TIME YOUR NOTIFICATIONS CAREFULLY

Timing matters, and we recommend you act quickly.

- Send a notification as soon as you become aware of the third-party breach or malware exposure
  - This gives you and your consumers time to change the compromised password on any and all accounts where it has been used
- Consider your customers' geographic locations and batch the sends based on their respective time zones

3 INFORM YOUR FRONT LINES

To keep both internal and external friction minimal, prepare your teams accordingly.

- Ensure your helpdesk and/or customer service teams are prepared to handle a potential influx of calls and emails they may receive from users about the communication
  - Be sure to train them about how to help consumers with next steps
  - Arm them with a script to follow with additional details that may have not made it into the communication you would have sent out
  - Provide them with a copy of the email going out, along with a playbook of what to say and do (and what not to)
- Consider a phased approach if you'll need to reset a large number of accounts
  - Tier is based on urgency from highest risk to lowest as to not overwhelm your frontline teams (which could increase call wait times and introduce great friction into the process for everyone involved)

4 INFORM YOUR CUSTOMERS

This step involves some decision-making, so be sure to think through what your email communication will say.

- Decide how transparent you want – and need – to be about what you know
  - SpyCloud provides the full context of each breach and malware record, including the source and description of the breach or malware infection, and often the plaintext password, so you may have more information at your disposal than you want or need to communicate
- Plan out how to guide your users on their next steps

CHOOSING YOUR TRANSPARENCY LEVEL

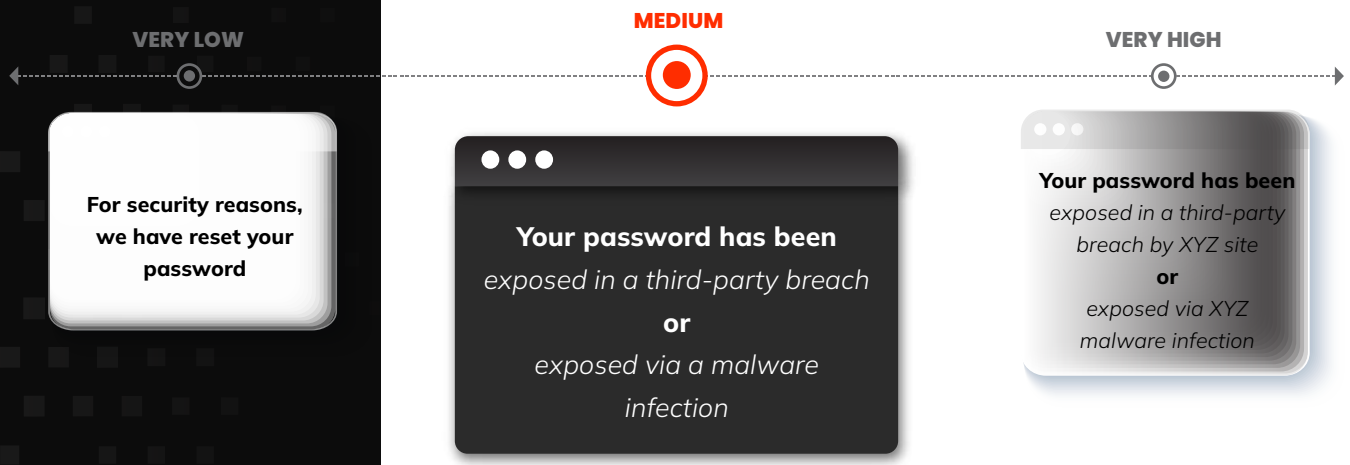
Choosing a more transparent message arms your customers with the information they need to secure any other online accounts that might use the same password. Knowing more detail about their exposed account may lead them to choose a stronger password or take other security precautions. A message of this type may also include information about the potential risks of account takeover:

- Exposure of personally identifiable information like addresses, credit card number and social security number
- Takeover of other accounts that use the same or similar password

At the same time, the transparency may raise additional questions that your support team may not be equipped to handle. For example: if you name the site or service that was breached, you may receive inquiries related to that site that your front lines may not be able to answer without creating additional training materials or standard responses.

Choosing a less transparent message may cut down on user concerns, but leaves the consumer more vulnerable to account takeover across their other online accounts. In addition, an uninformed user may be more inclined to choose a variation of an already-exposed password to replace the previous one because they underestimate the seriousness of the exposure.

Whichever level of transparency you choose, we do not recommend understating the risk. We have seen some companies deploy notifications that suggest the encryption method for a set of breached passwords cannot be hacked, and that the company "does not believe" that users' passwords were exposed. The purpose of your breach or malware notification should be to prompt users to implement a more secure, previously-unused password to protect their accounts from fraudulent actions or purchases.



BE CLEAR ABOUT NEXT STEPS AND THE DESIRED OUTCOME(S)

Write the email notification with the desired outcome in mind. If you are asking the user to reset their password immediately, we suggest laying out the step-by-step process in bullet form.

EXAMPLE

- Visit the example.com homepage
- Click <x> button at the <exact location on the homepage>

...and so on.

You may also want to include steps for enabling multi-factor authentication, and you can go a step further to provide guidance for choosing strong passwords – for example, **NIST password standards**, which require passwords no less than 8 characters and without repetitive characters, dictionary or context-specific words (like the name of the website being in the password).

BEST PRACTICES

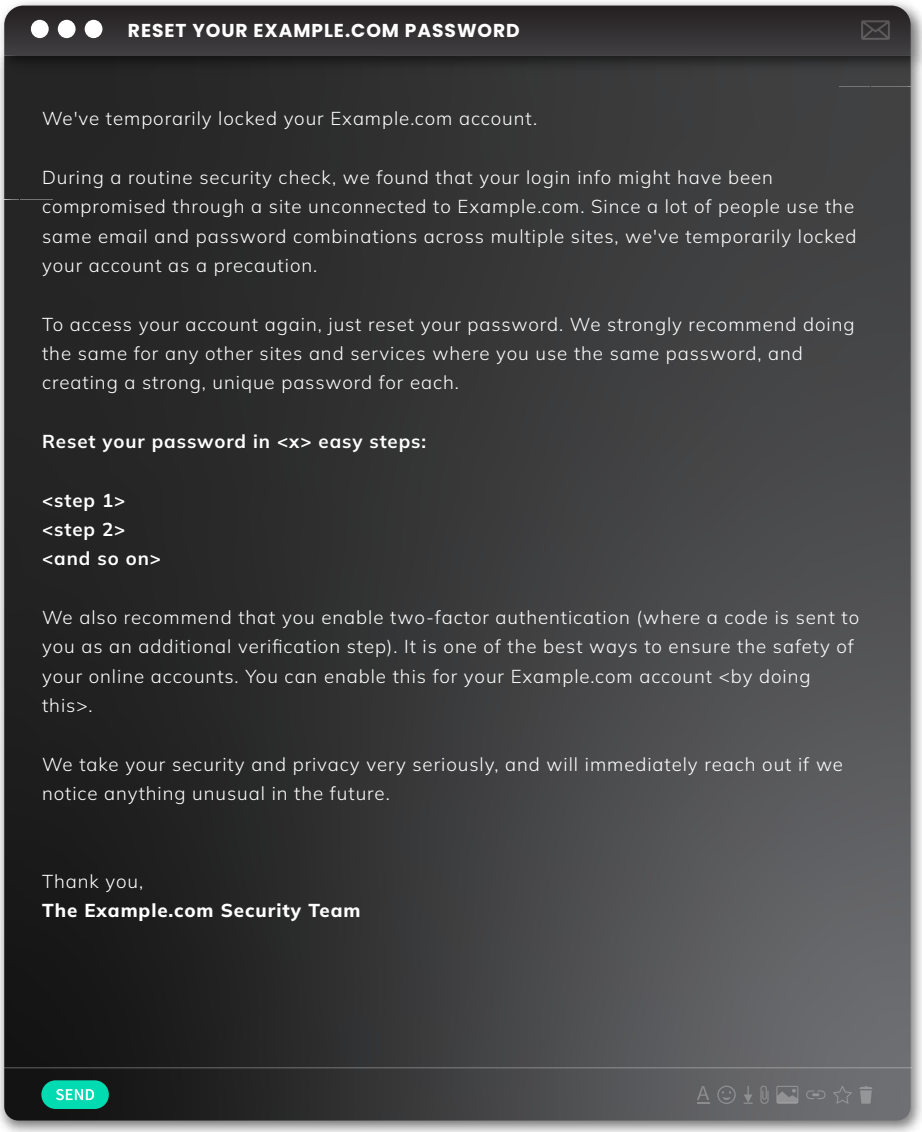
Avoid using hyperlinks: It's best to keep the email link-free to avoid coming across as a phishing attempt.

Be specific: Provide step by step instructions and a clear call-to-action.

Skip personalization: Your user may already feel exposed by the breach, so leave out the typical first name personalization.

SAMPLE EMAIL
THIRD-PARTY BREACH EXPOSURE

Below we have provided a well-crafted email notification for you to use as a starting point:



SAMPLE EMAIL
EXPOSURE VIA MALWARE INFECTION

Below we have provided a well-crafted email notification for you to use as a starting point:

RESET YOUR EXAMPLE.COM PASSWORD

Hi [CUSTOMER NAME],

During a routine security check, we found that your login might have been compromised by a malware infection on your machine. We do not have access to your machine to confirm this; however, your data was found in malware traffic collected by one of our cybersecurity partners. This indicates that your login details need to be updated to protect your Example.com account. But first, we recommend installing antivirus protection from a reputable provider <such as>, running a scan to clean your machine, and only then resetting your password on Example.com.

After running the antivirus scan, reset your password in 3 easy steps:
1. Go to Example.com
2. Where you would normally click to sign in, click "Forgot Password?"
3. Create a new, strong password that is unique to your Example.com account

We also recommend that you enable two-factor authentication (where a code is sent to you as an additional verification step) to ensure the safety of your online accounts. You can enable this for your Example account under your Account Settings.

It's possible that the malware may have compromised your login credentials for other sites as well. We strongly encourage you to follow the steps above for any other sites and services you use online, and create a strong, unique password for each.

We take your security and privacy very seriously, and will immediately reach out if we notice anything unusual in the future.

Thank you,
The Example.com Security Team

SEND

THE SPYCLOUD DIFFERENCE

THE RIGHT DATA, AT THE RIGHT TIME

SpyCloud's **Consumer Risk Protection** solution draws on the largest repository of recaptured stolen data in the world to help you make sure your customers are who they say they are. We enable enterprises to detect and automatically mitigate identity exposures early – negating the value of breached and malware-exfiltrated data before criminals have a chance to use it. Our customers continue to tell us their ability to prevent account takeover and online fraud hinges both on access to fresh, high-quality data and the ability to make that data operational through powerful automation.

To learn more, visit **spycloud.com**.

> "WE USE A NUMBER OF TOOLS TO CROSS-CHECK DATA, AND WE CONSIDER SPYCLOUD AS A TRUSTED RESOURCE FOR ANY TYPE OF INCIDENT THAT MAY IMPACT OUR CONSUMERS"
>
> *SECOPS MANAGER*
> **LENDINGTREE**