WHITEPAPER

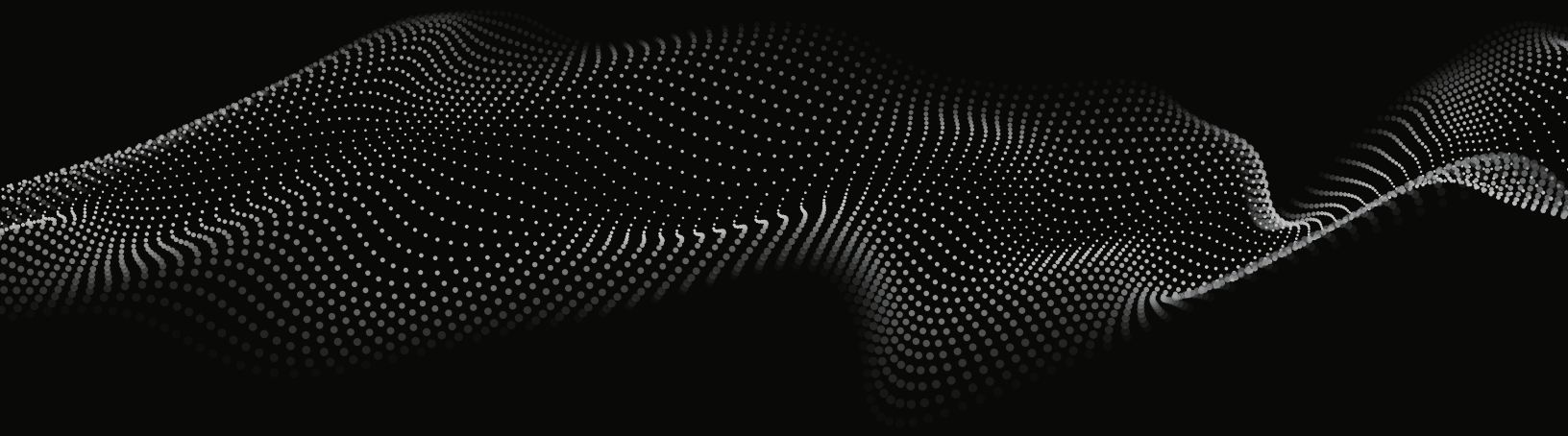
Best Practices:

Notifying Consumers of a Third-Party Breach

SpyCloud

SpyCloud

Table of Contents



Overview

It's no longer a question of 'if,' but 'when' – your consumers will reuse passwords, and those passwords will be exposed in a data breach. As soon as reused passwords become available to cybercriminals, your consumers are at high risk of account takeover fraud, which can result in substantial losses for you and for your consumers. With access to user accounts, cybercriminals can easily drain funds, siphon loyalty points, and make fraudulent purchases using stored credit card details.

SpyCloud enables you to protect your consumers from account takeover by proactively identifying passwords that have been exposed to cybercriminals in third-party data breaches. By validating your users' identities and resetting compromised consumer passwords promptly, you can lock out potential attackers before they have a chance to commit fraud.

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 fear or friction, you'll need to craft effective communications that fit your brand and inspire confidence. Based on input from SpyCloud customers, this playbook covers best practices for identifying your consumers' information in third-party breaches, 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.

Identify Affected Consumers

First order of business: identify and export the list of affected accounts. If it's just a handful of accounts, some organizations prefer to have a support leader email the consumers directly with a personal note, along with next steps. This avoids the complication of having to pull multiple teams together to produce and send a mass email. But in most cases, we're talking about a large list of compromised accounts. Ensure those email addresses are in your CRM or marketing automation system. You'll likely need your marketing team's help to launch a mass user communication; while they can help wordsmith an email, we have provided some example text later in this document.

Time Your Notification Carefully

We recommend sending the notification as soon as you become aware of the third-party breach. This buys your users time to change the compromised password on any other accounts where it has been used. Another point to consider is your consumers' geographic locations. Sending waves of alerts might be best, set to arrive in their inboxes at an appropriate time for their respective time zones.

Inform Your Front Lines

You'll want to ensure your helpdesk or customer service teams are prepared to handle the influx of calls and emails you may receive from users about the communication and understand their next steps. Callers may have specific questions about their accounts and whether their information was compromised. It's best to arm the teams with a script to follow with additional detail that may not have made it into the email you're sending. 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. While communicating urgently with affected accounts is important, so is not overwhelming your frontline teams (which might increase call wait times and introduce even greater friction into the process).

Inform Your Consumers of What Happened

Time to think about what your email communication will say. There are some choices you'll need to make upfront, including how transparent you want to be about what you know. Since SpyCloud provides the full context of each breached record, including the source and description of the breach, and often the plaintext password, you have more information at your disposal than you may want to communicate. And you'll have to decide how to word the users' next steps.

Choose Your Transparency Level

Choosing a more transparent message arms your consumers 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 is not 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 and 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 a few companies deploy notifications that suggest the hashing function for a set of breached passwords cannot be cracked, and that the company "does not believe" that users' passwords were exposed. The purpose of your breach 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 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:

1. **Visit the example.com homepage**
2. **Click <x> button at the <exact location on the homepage>**

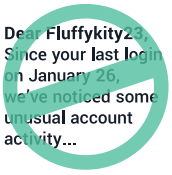
...and so on.

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.

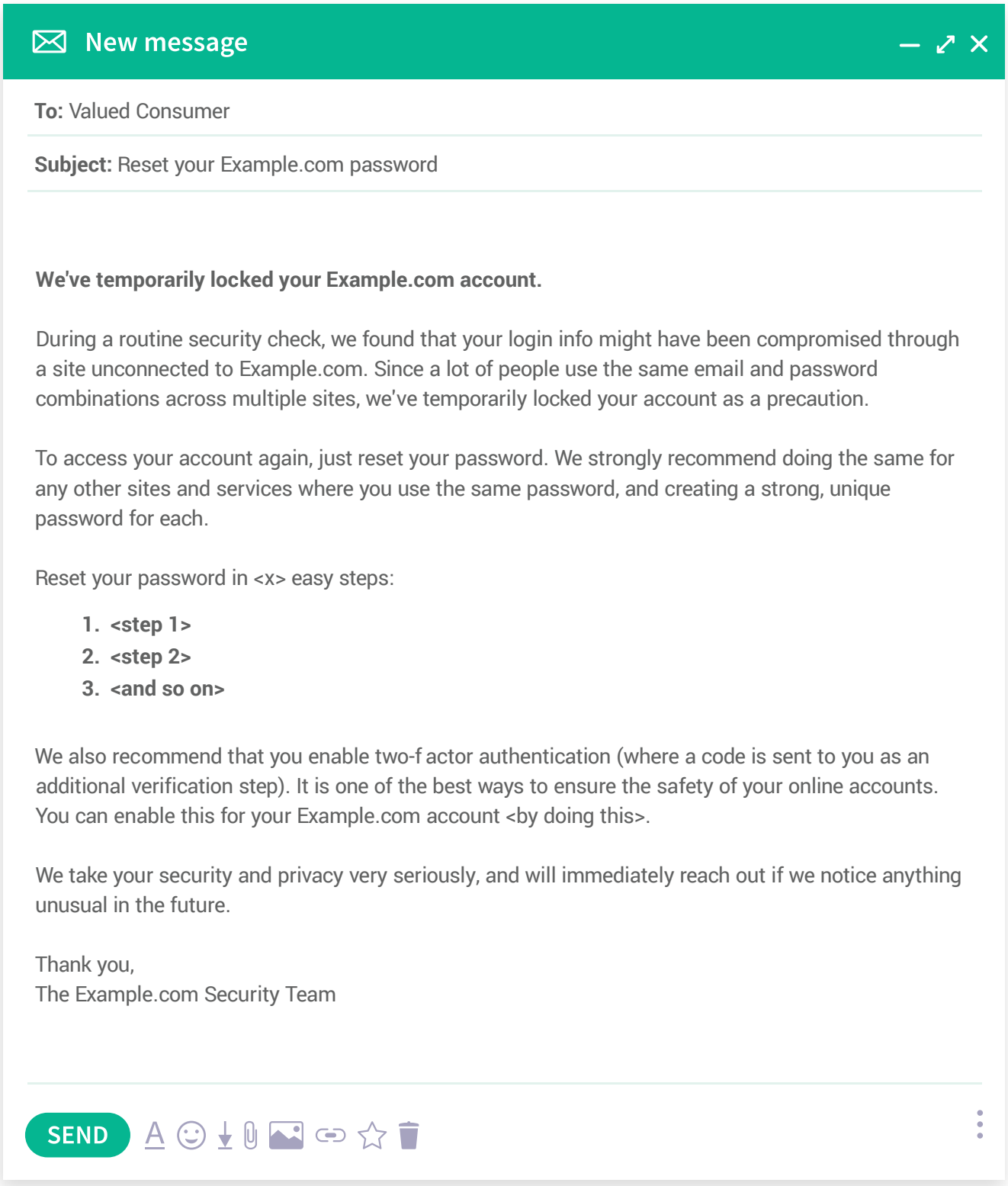
Be Specific
Provide step-by-step instructions and a clear call-to-action.



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

Sample Email

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



New message

To: Valued Consumer

Subject: Reset your Example.com password

We've temporarily locked your Example.com account.

During a routine security check, we found that your login info might have been compromised through a site unconnected to Example.com. Since a lot of people use the same email and password combinations across multiple sites, we've temporarily locked your account as a precaution.

To access your account again, just reset your password. We strongly recommend doing the same for any other sites and services where you use the same password, and creating a strong, unique password for each.

Reset your password in <x> easy steps:

1. **<step 1>**
2. **<step 2>**
3. **<and so on>**

We also recommend that you enable two-f actor authentication (where a code is sent to you as an additional verification step). It is one of the best ways to ensure the safety of your online accounts. You can enable this for your Example.com account <by doing this>.

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

SpyCloud

Conclusion

Third-party breach notifications are becoming more commonplace as service providers implement solutions to keep consumers safe from account takeover and avoid costly consequences such as fraudulent transactions. While these emails require careful thought and pulling together multiple departments to accomplish, if done right, they can also engender trust between you and your users.

The SpyCloud Difference

Building a security program around technologies that proactively leverage data acquired through Human Intelligence (HUMINT) tradecraft very early in the breach timeline is a critical path to success. SpyCloud's solutions, backed by the world's largest repository of recaptured credentials and PII, is an important layer of defense for cyber attacks that leverage stolen data. We enable enterprises to detect and automatically reset compromised passwords early and invalidate compromised web sessions, negating the value of breached data before criminals have a chance to use it.

Our customers continue to tell us their ability to prevent account takeover, ransomware, and online fraud hinges both on access to relevant data and in being able to make that data operationally actionable through automation.

250+ Billion
Recaptured Assets

25+ Billion
Total Passwords

30+ Billion
Email Addresses

Enterprise Protection

Prevent account takeover that can lead to ransomware.

Learn More

Consumer Protection

Combat account takeover and online fraud.

Learn More

Investigations

Unmask criminals attempting to harm your business.

Learn More

Data Partnerships

Enhance your solution with SpyCloud's data.

Learn More

SpyCloud