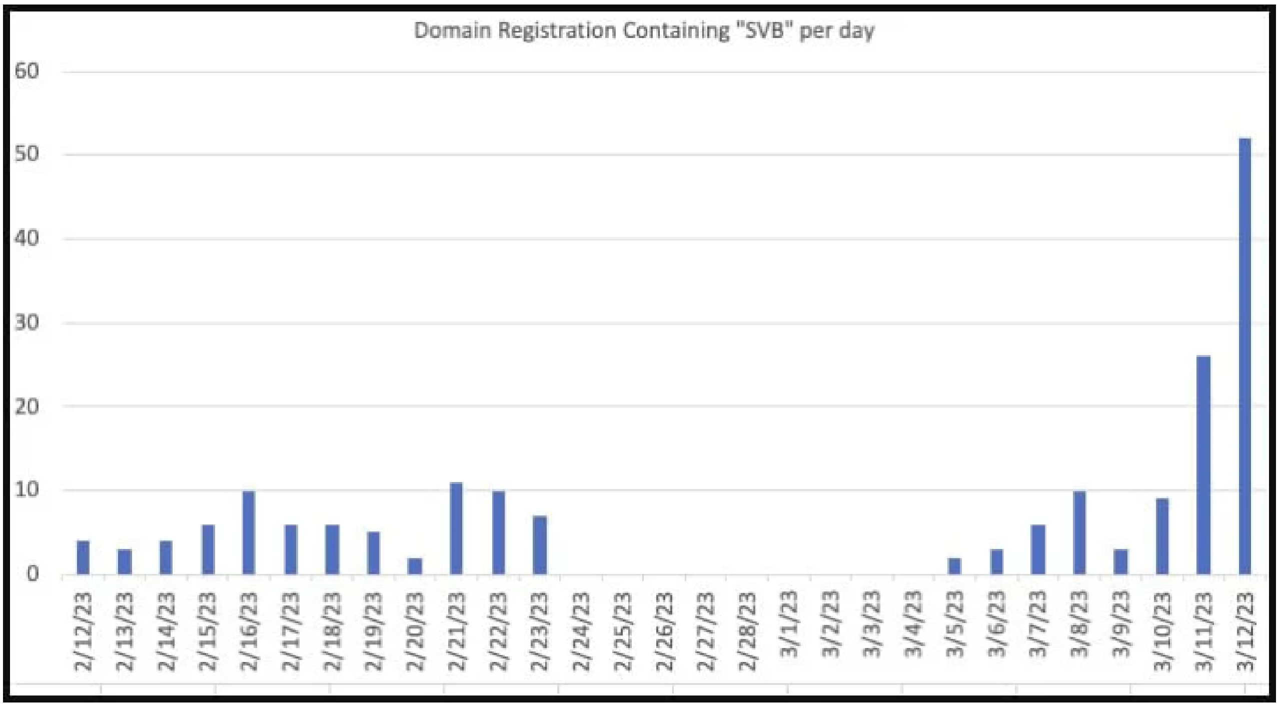
CYBER ALERT:
HOW CYBERCRIMINALS EXPLOIT BANK FAILURES TO STEAL MONEY & DATA

First it was Silicon Valley Bank, and then it was Signature Bank – the news of these two major bank failures has sent shockwaves of concern in the United States and globally that we're inching closer to a recession. Given the prolonged, high levels of inflation we've seen recently and reports that other financial institutions, such as Credit Suisse and First Republic are struggling, it's easy to understand why people are worried.

It's in moments fueled by uncertainty and panic, such as these, that cyber scammers thrive.

It's in moments fueled by uncertainty and panic, such as these, that cyber scammers thrive. For them, tragedy and bad news present an opportunity to prey on people's emotions. In fact, according to Cyble Research and Intelligence Labs, since the recent bank collapses, many suspicious web domains have surfaced, including:

- svbcollapse[.]com
- svbclaim[.]com
- svbdebt[.]com
- svbclaims[.]net
- login-svb[.]com
- svbbailout[.]com
- svb-usdc[.]com
- svb-usdc[.]net
- svbi[.]io
- banksvb[.]com
- svbank[.]com
- svblogin[.]com



In light of recent events, everyone needs to be aware about potential scams, but especially individuals and organizations that were clients of these banks. Here's what you need to know about how bad actors design scams in moments of crisis, and what you can do to stay vigilant.

THE SCAMS

Bad actors are using the current market environment to push out a wave of attacks surrounding the financial space, including phishing, spear phishing, social engineering, and business email compromise. Scammers have been creating deceitful emails and texts posing as the collapsed banks, telling recipients of these messages that their funds have been frozen to create a sense of urgency. Bad actors may also pretend to be someone from your organization, such as the CEO, impersonating them via email, text, or social media. They have also been reaching out to people under the guise of providing legal services, loans, support packages, or other fake services related to the bank's collapse.

Scammers might then ask the targeted person to do several things, including the following:

- Click on a compromised link.
- Provide personal information, such as name, phone number, email, account balance, login credentials, and other data.
- Transfer money to a new account to avoid the loss of funds, when in reality the funds would get transferred to the scammer's account.

Cybercriminals are savvy, using their technical and investigative skills to craft personalized messages so that they're able to gain a person's trust for their benefit. Their communications will often contain convincing details, such as the bank's logo, a plausible web domain, and a known executive's name to obtain that trust.

Bad actors may also choose to exploit their winnings from previous phishing scams or data breaches to attempt targeted, volume driven credential stuffing to gain access to accounts. In the midst of so many developing events, be on the lookout for suspicious transactions and transfers.

OUR RECOMMENDATIONS

Though cybercriminals are innovative and persistent with their attacks, being educated and prepared is a viable line of defense against their tactics. Here are some indispensable cybersecurity best practices you and your employees should follow at all times, but especially in times of turmoil:

- Continuously train and educate employees to be able to identify and report threats, like phishing or unsafe, suspicious URLs.
- Confirm the authenticity of links or email attachments before opening them, preferably via a verified phone number, as an email account may be compromised. It is always best to visit the verified website to ensure that you are calling the correct number, and not an impersonated one that may be in the email.
- Don't download files from unknown websites.
- Employ Multi-factor Authentication for all users.
- Have encrypted backups of all data.
- Use an Endpoint Detection and Response solution to monitor and stop suspicious activity.
- Enable and analyze logs for your devices and digital landscape.
- Have an incident response plan and ensure it's up to date.
- Use cyber security controls, like anti-virus and firewall software.
- Review your cyber insurance to ensure that you're covered for cyber incidents should they happen.

Many companies and individuals have been impacted by recent events in the banking world. It's an unfortunate reality that bad actors will try to capitalize on the uncertainty for their gain, which means you need to do your part and be prepared to prevent their attacks. If you have yet to do so, now is a great time to assess your cyber risk, security posture, and insurance coverage should disaster strike.

Contact us about how to best implement an effective cybersecurity training program and for guidance about your cyber insurance coverage needs.

Contact Us

This material has been prepared for informational purposes only. BRP Group, Inc. and its affiliates, do not provide tax, legal or accounting advice. Please consult with your own tax, legal or accounting professionals before engaging in any transaction.