In this issue:

- **Hack-Proof Your 401(k) Account**
- **Savvy Cybersecurity quick links**
- **Cybersecurity shorts**
- **Software updates**

**The following content is provided courtesy of Horsesmouth, LLC, and provided courtesy of Miles Harris.*

This month we'll be focusing on how to protect your retirement accounts from hackers. Read on for more information on 401(k) theft, as well as:

- Why you must look carefully at links shared via Slack
- A breach at the new social media platform, Clubhouse
- And much more

Hack-Proof Your 401(k) Account

Americans hold over $20 trillion in 401(k)s and other retirement accounts—yet federal safeguards to protect these accounts from theft are lacking. Cyber thieves have begun targeting retirement accounts more frequently in the past few years. While there is not a lot of public data on retirement account theft, The Wall Street Journal reported on lawsuits by account holders looking for reimbursement of 401(k) accounts.

In 2019, Heide Bartnett discovered $245,000 was wrongfully distributed from her 401(k) after receiving a statement in the mail. Bartnett believes that a hacker was able to access her account online, possibly using the Forgot Password feature, where they added their address and bank account information. The scammer was then able to initiate the distribution to the bank account they owned.

Bartnett filed a lawsuit against Abbot (her former company) and Alight Solutions, the benefits administrator. She was able to recover part of the distribution through taxes withheld and from the fraudulent bank account, but she is seeking the full balance plus damages. Bartnett had to continue working longer than anticipated and has affected her thinking about retiring for good.

Currently, consumers have better protection for their savings accounts and credit cards. The Government Accountability Office (GAO) has requested that the Labor Department improve protections for 401(k) investors.

According to the GAO, cyberattacks on 401(k) providers could lead to "severe financial ramifications." The Labor Department currently does not have minimum security requirements for plan providers. For now, your clients must take security into their own hands.

Savvy Cybersecurity actions

There are steps you can take to help protect your retirement accounts from being hacked. Many of the Savvy Cybersecurity principles can be applied to these types of accounts for better protection.

1. **Set up an online account**

First, be sure you set up an online account with your 401(k) provider. This will allow you to access your account more easily and will also ensure that an impersonator cannot make an account in your name. Of course, when making your account, there are cybersecurity best practices you should follow to keep it secure.

2. **Use a strong and unique password**

When setting up your online account, you must create a good password. Do not use a password you have used elsewhere. Follow our password advice from the Savvy Cybersecurity program, such as using a mnemonic password or a goal-based password.

3. **Enable two-factor authentication**

In addition to having a unique password for your account, you must also enable two-factor authentication. Two-factor authentication protects your account even if a hacker has your password, they will still need the one-time security code to access your account.

If your 401(k) provider does not offer two-factor authentication, raise the security issue to them. Any sort of financial firm should be offering this level of security.

4. **Check accounts regularly**

Lastly, check your account regularly for any unusual activity. If your provider offers text or email notifications, sign up for those so you are notified any time a change is made to your account. At the very least, you should log into your account monthly to check your balance and contact information.

Cybersecurity shorts

Attention Clubhouse users: 1 million accounts leaked. Cybernews reported that personal data for around 1.3 million users of the recently popular app, Clubhouse, was scraped and posted on a hacker forum. The compromised data included names and handles for other social media accounts.

Slack users: Beware of malicious links. According to CyberScoop, Hackers have been using Slack and Discord to distribute malware to unsuspecting victims. Suspected cybercriminals have been uploading files to the platforms, obtaining a link from that upload, and sharing the links outside of the two apps.

ParkMobile app exposes information on 21 million users. The popular mobile parking app appears to have been a victim of a data breach. Information such as email addresses, phone numbers, license plate numbers, mailing addresses, and more are now for sale online. ParkMobile believes the incident occurred due to a security vulnerability in third-party software. If you use the ParkMobile app, you should change your password immediately.

Biden's Covid-19 relief bill offers a cybersecurity strategy. President Biden signed a $1.9 trillion Covid-19 relief bill into effect and set aside $1 billion for the Technology Modernization Fund (TMF) and millions more for cybersecurity. These funds came at a crucial time following the SolarWinds attack, which highlighted the vulnerabilities of many federal agencies.

Financial industry preps for proposal requiring 36-hour breach notification. An initial proposal mandates that financial firms would need to report more kinds of cyber incidents to regulators within 36

hours. Among the proposed rule's provisions is that bank service providers would have to provide notifications to banking organizations when they suffer damaging cyberattacks. CyberScoop goes into great detail about the proposal, what the 36-hour breach notification will mean for different sectors of the financial industry, and more.

FBI has new advice for ransomware attacks. A new two paged document released from the National Cyber Investigative Joint Task Force strives to help organizations guard themselves against a persistent and dangerous cybersecurity threat, ransomware. In this interview,a Secret Service Deputy Director Greg McAleer and FBI Cyber Division Unit Chief Ryan Pierrot speak on the podcast Federal Dive with Tom Temin about the task force's work on this newly released document.

Is cybersecurity a priority of your business plan? The majority of modern business takes place online and good cybersecurity must be prioritized by business owners. Breaches and hacks make a poor impression on your customers and potential customers. Follow these cybersecurity tips to have a more secure business.

What is the history of women and cybersecurity? Today, women comprise 24% of the cybersecurity workforce. However, the industry is still in need of a large and diverse community because the answer to safer computing is having a diverse workplace. Diversity brings different perspectives and fresh outlooks to the table, which can change the status quo. Learn more about why diversity is crucial in the cybersecurity industry.

U.S. Intelligence report warns of increased offensive cyber operations. The U.S. intelligence community's Global Trends report noted that many offensive cyber operations will likely target civilian and military infrastructure. Additionally, over the next two decades, the intensity of competition for global influence is likely to reach its highest level since the Cold War. Read more about the report and what is expected over the next 20 years.

Software updates

Adobe: Adobe released updates this month for Photoshop, Bridge, RoboHelp, and Digital Editions. If you run any of these programs, click here to learn more about the updates.

Apple: iPhone and iPad users should update their devices immediately to iOS 14.4.2 or 12.5.2. Apple has released these updates in response to a vulnerability that allows hackers to access private data via your web browser. Learn more about the update here.

Microsoft: Over 100 security vulnerabilities are patched with Microsoft's latest update. This includes security fixes for Microsoft Exchange Server which we covered in last month's newsletter. There are also updates for Microsoft Office products. Your device should prompt you to update automatically but you can learn more about the updates here.