In this issue:

- **How to fight back against common elder scams**
- **Cybersecurity shorts**
- **Software updates**

Dear <first name>,

Happy New Year! We hope 2020 is off to a strong start. For cybercriminals, there has been no break--we have already seen a handful of scams and hacks in the first month of the year. Read on to learn more about the cybersecurity happenings this month including:

- Important news for Windows 7 users
- A massive breach at Microsoft
- New ransomware threats
- And much more

How to fight back against common elder scams

Over two million elderly people fall victim to a scam every year—and experts think there are many more that go unreported. The elderly population has long been a target for scammers for many reasons. First, many are trusting and may have decreased cognition stemming from health issues. Scammers are also aware that many of these people have retirement accounts with money to spare—or conversely, are on a budget and likely to jump on a chance at a windfall.

Reports find that elderly fraud is now a multi-million dollar business, with the median amount lost by someone over 80 being $1,000. There are many types of scams that are targeted at the elderly, and awareness is the first step in protecting yourself or loved ones. Here are some of the most common elder scams to know.

1. **Medicare and Social Security Scams**
   Scammers misrepresent these government programs to trick elderly victims into sharing personal information. In some cases, they may pretend to be a Medicare representative and ask for the victim's information and Medicare number, which is then used to commit fraud. In other cases, they may ask for their bank account information to steal money from the account.

   The same has happened with Social Security--many scammers pose as representatives who promise to improve benefits. They may ask the victim for money for these services or may get enough information to have the benefits deposited in their accounts.

   What to do: It is important to know that Medicare and Social Security will never call you to sell you anything. The agencies will also not contact you for personal information unless you have called them first. If you are unsure, hang up and call the agencies directly. Also, be sure to check Medicare and Social Security statements regularly for anything unusual.

2. **Sweetheart Scams**
   Unfortunately many lonely or widowed elderly people fall victim to sweetheart scams every year. Here, scammers pose as a love interest online. They form a relationship with the victim virtually, expressing their love&hellip;and then ask for money. Since the relationship is already been established and the victim sees this person as a boyfriend or girlfriend, they often send the money. By the time a family member intervenes or the elderly person realizes their paramour is a fake, it is very difficult to get the money back. Often the amount of money sent can total thousands of dollars.

   What to do: If you meet someone online, it is important to find out if they are who they say they are. It is a red flag if an online friend does not want to meet in person or use video chat. If you think a loved one has fallen victim to this scam, be empathetic and try to ask more questions. Asking for power of attorney can grant you easier access to the accounts to check for anything suspicious.

3. **Phishing and Telemarketing Scams**
   More generally, elderly people are often victims of various phishing and telemarketing scams. Usually, these scams, whether they are via email or over the phone, ask victims to share personal information such as name, address, birthdate, banking information, and more. The scammers can then use this information to impersonate the victim or steal funds. Elderly people who are not comfortable with the computer may be quick to click on malicious links that download malware or expose information.

   What to do: If you receive a phone call asking for personal information, think twice before sharing. If you are unsure, hang up and call the institution directly. When using email, do not click on any links or open attachments in an unsolicited email. Even if you think you know the sender, think twice before you click. If you are concerned about a loved one being scammed, educate them on how to check emails for fraudulent links.

Cybersecurity shorts

Another cloud-hosting company hit with ransomware affecting thousands of customers. Synoptek, a California based IT management company, became victim to a ransomware attack last month. The company provides cloud services to many industries including local governments, financial services, healthcare, software and more. Synoptek has paid the ransom, according to sources. This news follows reports that two other cloud hosting companies suffered ransomware attacks last month.

FBI warns of Maze ransomware making the rounds. This strain of ransomware uses a variety of, methods for intrusion, including the impersonation of government agencies and security vendors. Maze was first discovered in November 2019, but has infected many companies since. As always, it is important to closely examine emails before clicking any links or opening any attachments.

Amazon defends Ring's security policy following "hacks" last year in new letter to U.S. Senators. As you may recall, many Ring users reported their smart doorbells being hacked late in 2019. Ring explained that many of the incidents stemmed from poor password use, but many experts noted that two-factor authentication was not the default on the device. In its letter to senators, Ring said it will prompt users to set up two-factor authentication and continue penetration testing.

Hackers are scamming telecom employees to take over customer phone numbers, according to a new report. As more employees and consumers become aware of the SIM swapping scam which allows hackers to take over a victim's smartphone by impersonating the customer to telecom employees—hackers have found a new method. Now, the hackers pretend to be IT workers needing to fix something on a telecom employee's work computer. After they trick the employee into allowing control of their computer, the hackers are able to take control of customers' numbers.

Over one billion medical images are at risk of being exposed due to insecure storage systems. According to experts, hundreds of hospitals, medical offices, and imaging centers may be at risk of exposing these images. The issue was discovered last year after 24 million patient exams were discovered online. Despite warnings, many hospitals and medical offices have not secured systems.

Vulnerability in Citrix VPN software leaves users at risk. Security experts discovered the issue weeks ago and it could allow hackers access to networks that use the service. Many corporations use the Citrix VPN and it is estimated that tens of thousands of companies could be affected. Citrix is currently working on a permanent patch for the flaw.

Microsoft no longer supporting Windows 7—what you need to know. As of January 14, devices running Windows 7 will no longer receive software updates that could offer protection from malware and viruses. Microsoft technicians will also no longer offer technical support for those devices. If your device is less than three years old, you can upgrade to Windows 10 for $139. If your device is older than three years old and running Windows 7, Microsoft recommends buying a new computer.

iPhones can now be used as security keys for two-factor authentication as part of Google's Advanced Protection Program. This is considered one of the most secure two-factor authentication methods today because you need access to the physical device. Security experts say that text message two-factor authentication codes can be intercepted by hackers. Android users have been able to use their device as a physical security key since last year. Google's addition of iPhones to the programs will allow more people to improve their security.

250 million records exposed in Microsoft data breach. The company announced that a customer support database was visible online for the month of December. The database contained conversations between support agents and customers covering a 14-year period. Microsoft will notify those who were affected.

iPhone 11 users can now have better control over their location settings. Security writer Brian Krebs first pointed out the issue last month when he discovered the iPhone 11 users' locations were queried even when applications were set to not request this data. The new phones included a setting called Ultra Wide

band that allowed users to share files locally with nearby phones. iPhone 11 users can now disable Ultra Wideband.

Beware of FedEx phishing scam making the rounds. Consumers have reported receiving fake text messages and emails from FedEx alerting them to a package. The messages contain a tracking code and ask recipients to click on a link to set delivery preferences. The link allegedly sends people to an Amazon survey and asks for a credit card number to claim a free product. FedEx says the messages are not legitimate.

Jeff Bezos' smartphone was allegedly hacked by a malicious video file sent from a WhatsApp account associated with Saudi Crown Prince Mohammed bin Salman, according to a new report. The report was produced by FTI consulting, a Washington firm that reported medium to high confidence that the hack occurred after a video file was sent to Bezos' phone via WhatsApp. Saudi Arabia has denied the allegations.

Software updates

Firefox: Firefox users should update their browsers immediately following a critical zero-day flaw. The security issue has been used in targeted attacks in the wild. Your browser should prompt you to update automatically but you can check to see if you are running version 72.0.1 in the Help area of Firefox.

Microsoft: Microsoft has released updates to patch 50 security issues in Windows 10 and other Microsoft products. The final patch for Windows 7 was also released this month. As discussed earlier, Windows 7 users should upgrade their operating system or device. You can read more about the updates here.