**Text of video recording** (from AI prompt)

The particular one you mentioned where it’s a text message that just says, “Hello,” is just hoping that you will reply so they can engage you. Eventually, they’ll get around to making you some kind of offer or asking you for information. When you get these random texts, just like the phishing emails that we see so much, just discard it or block it, but do not reply to it.

Let’s talk about some other defensive measures that we can take for phishing. The bad guys are trying to trick us into doing something that we wouldn’t otherwise do, like wiring money somewhere, and they’re very good at it. Our parents taught us to trust people, and the scammers are trying to take advantage of our trusting nature.

In the case of the scam that we just talked about, they use several different techniques to gain our trust. One red flag is that they contacted us; we didn’t contact them. Secondly, they pretend to be an authority figure like a Big Sir, and they say this is an urgent situation that has to be resolved very soon. They want to convey that sense of urgency to increase our emotional response. Eventually, they will ask us to send money, probably through a method that legitimate businesses rarely use for payment, like wire transfer, gift card numbers, or cryptocurrency like Ethereum or Bitcoin. Venmo and Zelle are peer-to-peer methods, and when you hear a request from Venmo or Zelle, that’s probably another scam. An envelope full of cash is another red flag.

So someone earlier asked about an example of a phishing email, and here’s one. I haven’t seen the one in the branch, but this is similar to the kind that we receive every day in our email inbox. You’ll notice at the top, the text says that my Facebook has been hacked, and in order to reinstate my account, I should either complete the attached form or click on the link below. Sounds pretty legit, right? But there are some red flags. Most importantly, the sender’s name here is “Facebook Support” right up at the top, but the sender’s actual email address is not from Facebook.com; it’s from aiken.co.uk, and clearly, that is not Facebook.

So this is the first thing that we should check when we get an email—make sure it’s really from the email address that matches up to the name. This email address may not be visible on a mobile device like a phone or a tablet, so if in doubt, set that email aside until you can check it out on your computer. Mobile devices have kind of a smaller screen size, so they’re not able to present everything to you this way. But check it out; don’t reply to it. Scammers can even spoof the email address itself, so check out any clickable links. For example, if you mouse over that link that says your Facebook profile, it causes the real Internet address of where you’re going to go when you click that link to appear at the bottom of the screen. Again, this is not a Facebook website; it’s http://deviate-something.

Similarly, like the earlier one, you can’t do this on a phone or a tablet. So if in doubt, set that email aside until you can check it out on a computer. Lastly, you’ll notice that there’s an attachment, which is a zip file, and that may be hazardous unless you really know what it is. So if you see these red flags, it’s probably a scam, and your best approach is to just discard it.

Passwords can be a real pain, especially on a website that requires a special symbol in the password. So let’s talk about the difference between weak passwords and strong ones because this can make a huge difference in the security of your personal world.

There’s a story about what happens when you use an easy-to-remember password. Last summer, I got an email from my friend Tom asking if I could do him a favor and buy some gift cards for him and send the numbers to a different email address. He’d pay me back when he got into town. Does this scam sound familiar? Yeah, there’s a lot of it going around. Well, Tom had an easy-to-remember email password, and that enabled a scammer to get into his email account. Then the scammer sent that email from Tom’s email account to everyone in his address book, so it looked like the email came from Tom because it came from his account.

Tom didn’t even know that a scammer was sharing his email account until I contacted him. I got one of those emails, and he called his email provider and tried to get control of his account, but he couldn’t prove to them that he was the real owner of the account. In the end, the email provider left the account in the control of the scammer, and Tom had to start an altogether new email account. What a mess! And then it got worse. He got phone calls from two of his friends; they had bought the gift cards just as he’d asked, and they had sent the numbers to that other email account. They were wondering when Tom would reimburse them for the cards.

Tom was understandably embarrassed that he had allowed his friends to be defrauded, and he wanted to notify everyone in his address book about the scam, but meanwhile, the scammer had deleted his address book, so he didn’t even have his friends’ email addresses anymore. Fortunately, this didn’t go into complete identity theft, but the whole mess happened because Tom had an easy-to-remember but weak password.

So what makes a password strong rather than weak? Today, a password should be at least 12 characters long. But automated word list searches make it possible to guess a dictionary word almost instantly. How about substituting numbers and symbols for letters? Not at all, because the bad guys aren’t trying to crack your password manually; they have programs that do it for them, and their automated word lists for cracking passwords already include these character substitutions.

How about completely random characters and special symbols? This 8-character password could be cracked in about 40 minutes. Better than instantly, but really not good enough. That’s why I suggest that you need at least 12 characters. The best approach is to use a passphrase. A passphrase is a set of random words, like in the example “correct horse battery staple,” which is 25 characters long. It would take decades to crack, and it’s easy to type. Of course, many websites require that you use a capital letter, a number, or a special symbol, so consider using passphrases like this to protect your accounts.

Using the same password for different accounts is a bad idea. Remember my friend Tom, whose friends got scammed because he used a weak password? Tom made another mistake: he used the same password on other accounts, including his bank account. The scammer now had not only access to his email address and all his friends, but also access to Tom’s bank account. When he told me this, I drove him to the bank, and we got that fixed at his bank before the scammer could empty his account.

Using a password in two places is a bad idea for another reason: servers are frequently breached. In recent years, the passwords for Facebook and Yahoo sites have been stolen. If you have an account on one of these sites that was compromised, the bad guys now have your password, and if you reuse that password elsewhere, they have all they need to take over that account as well. So, don’t reuse passwords.

Many websites encourage you to use single sign-on using Facebook, Google, Apple, or Amazon, and this seems convenient, but it’s yet another way that companies track you across different websites and then sell your information. It’s also risky because if the bad guys breach one of those sites, they have your password for multiple sites, not just one. So, avoid using single sign-on.

So what do we do with all those unique passwords that we’ve created? Before we consider where to store the passwords, let’s think about to whom the passwords are at risk—criminals out on the Internet or criminals in your house? Obviously, the criminals on the Internet are a much bigger threat than someone who’s broken into your house, so that gives us some direction on how and where to store passwords.

How about a file in your computer, maybe a Word document or a spreadsheet? If a bad guy out on the Internet is able to hack into your computer, he now has all your passwords. How about a sheet of paper in your desk drawer? That’s actually more secure because the bad guys on the Internet cannot see into your desk drawer. But there’s an even better solution: a password manager.

Password managers can generate a strong password or passphrase. It can store that password in an encrypted vault, and it can automatically fill that long password into your login screen and log you in. This makes it both easier and more secure. Finally, have you heard about passkeys? They’re a way to finally eliminate passwords by using a cryptographic token. This is just getting underway, but many big websites like Google and Facebook have made passkeys available. As the rollout progresses, we’ll be able to get rid of passwords. So, get started with a password manager now.

Even if you don’t recognize the term “two-factor authentication” or “multi-factor authentication,” you’re probably already using it. When you go to your ATM and put in the card, you also put in a PIN number, which is a kind of second factor. When a website sends you a six-digit code in a text message or an email, that’s another second factor.

It’s important to use two-factor authentication when you log into an account that you care about, particularly your email, financial accounts, and so on. Two-factor authentication adds a layer of security that can prevent 99.9% of account takeovers.

So far, we’ve talked about ways to avoid fraud at your branch and on your own devices. I want to thank you for joining in today because you are the ones who will make the difference in reducing fraud. I