[Golden1 podcast]

HOST

Hi everyone, welcome to this episode of the Golden 1 podcast!

Today's topic is something that hits home for everyone: digital banking and security.

In this age of digital banking, it's easy to take security issues for granted. Whether it's accessing your accounts through a website or making transactions with your phone, it all happens so effortlessly. We assume that our money is secure – and it is. Financial institutions in particular take your online security very seriously. However, that doesn't prevent thieves from trying to steal your money.

The good news is that you can stop them using a few simple best practices. And that brings us to the first part of today's show: security tips. Our first tip is one you've probably heard before, but it's worth repeating since it's likely the most effective way to protect yourself: use hard-to-guess passwords for your online accounts. Avoid obvious references such as your birthday, address, kids' names, and pets.

The best passwords use a combination of lower and uppercase letters combined with numbers and symbols. If you're struggling, think of details about yourself that not too many people know. And this is also important – don't use the same passwords over and over. If a crook cracks it in one place, he'll be able to invade all of your online accounts and apps.

Now some thieves are clever enough to take the information they can find about you and use it to guess your passwords. Which leads us to our next tip – be careful what you share about yourself in social media. Over-posting on Facebook, Instagram and Snapchat about people, places, and things that you love might tip off a hacker. If you want to select who can and can't see what you share, check the privacy settings on your account.

Our next tip has to do with public WiFi. Most of us use it because it's free and usually faster than your phone's data. The problem is that public WiFi is usually unsecure. That means that any information you enter is vulnerable to a motivated hacker.

So if you need to check your account balance, transfer money or do any of the other financial transactions that you're used to, wait until you have access to your own secure WiFi connection.

Finally, set up alerts for your different financial accounts. With alerts, you'll get notifications sent by email or directly to your phone updating you about certain activity. Want to know if a transaction was made on your debit or credit card? There's an alert for that. You can also stay in the know by setting alerts for when a security question is answered incorrectly, or if your account has been locked.

Okay, now that we've discussed how to protect online accounts, let's talk about how to avoid a scam, because the two often go hand in hand.

Although some of their tactics are easier to spot than others, all scammers seem to be after your money. The most common way they'll target you is through phishing. "What's so wrong with fishing?" you ask. "You get to enjoy the outdoors while communing with nature!" I'm sorry to say that this is phishing with a "ph," which is very different -- and much less enjoyable -- for you, the victim of the scam.

In a typical phishing scam, you'll get an email from someone you've never heard of asking you to click an important link. The problem is that once you click it, the link infects your computer with malware, which spies on your internet activity, including of course the passwords you use to access your online accounts.

This kind of scam is usually easy to identify, but some thieves are a little more sophisticated. They'll send you an email posing as a representative from, say, your financial institution or a credit card company. They'll tell you that, in order to confirm information about your account, they need you to provide your account number.

Pretty sneaky, right? Just remember that any reputable company will never ask for sensitive data over email. And if you receive a message that you're unsure about, research the company online or contact customer service to ensure that the correspondence is legitimate.

Another red flag to watch out for is fake retail websites. In an attempt to steal your card or account info, scammers will create a fake website advertising too-good-to-be-true prices on popular

products. So if you're shopping on a website that you're not familiar with, make sure you check the URL. If it starts with "https," it's safe. That "s" is important. It stands for "secure," and signifies that whatever data you enter is protected, and that the website owner obtained a special certificate to get it.

Our last scam tip is more of a good general rule of thumb, but it can help you stop an account hack before it wreaks havoc on your finances... Review your account activity regularly. It's easy to fall into the habit of only checking your monthly statement, but in the event that someone does access your information, you want to nip the fallout in the bud. That's why reviewing your purchases and withdrawals is so important. See something you don't recognize? Report it as soon as it happens. If it's the result of fraudulent behavior, you can lock down your account, and potentially reduce your liability.

Feeling a little more secure about your online security? Good, because we've arrived at the end of our show. Thanks for checking out this episode of the Golden 1 podcast!

[ALT: Thanks for checking out this episode of our podcast!]

###