Title: Think Twice Before You Swipe : Avoiding Fraud Online

Rich&Regular: Julien and Kiersten

Fraud can wreak havoc on your life. Whether you are trying to apply for a job, trying to get an apartment, or apply for a loan. If there is some type of financial fraud that shows up on your credit report, it can make living your life really, really difficult.

And one of the biggest challenges in dealing with fraud is that it's really hard to detect. Unless you're reviewing every line item of every statement and credit report, the actual fraud itself can occur and continue to occur without being detected. In fact, criminals do this intentionally so they can slowly commit the illegal act and fly under the radar over extended periods of time without detection.

So the first tip to helping to protect your accounts from financial fraud is to check your mobile banking or PNC app for irregular activity. Now, I know this can sound time-consuming, but the good news is, it gets easier over time. The more familiar you are with your spending habits, frequency of charges and budget, the more likely you are to notice when something looks a little off. If you're just starting out, we'd recommend you do this at least weekly to make sure you don't see any suspicious activity in your accounts. And assuming you have access to all your documents, it should only take you between 10 and 15 minutes. If you want to take this to the next level, then you should enroll in a credit monitoring service that alerts you whenever a new account is created. Also, you should set spending alerts on your debit card and credit card statements so you receive an alert whenever a charge of a certain amount is made on your accounts. That way, you know the moment it happens and can spring into action to stop it from happening again.

The second tip is to avoid making financial transactions or checking financial accounts while using public wifi or shared computers. This is critical for students if you're going to a lab, library, coffee shop, or any other public area where you're asked to log in. While there may be some security measures in place by way of usernames and passwords, most publicly available networks can easily be used to monitor your activity and steal your sensitive information. In some cases, this is done simply by looking at your screens. And in others, it can be done seamlessly using sophisticated tools and tactics to tap into your phone or laptop without you even knowing it's happening. So if you have to log into a public network, just be sure to use encrypted forms or be sure to use what are called VPNs, virtual private networks. These are networks within the public network that are out of the view of anyone who may be trying to steal your financial information.

Tip number three is to use paperless statements to avoid financial fraud. Whenever you're setting up a new account or managing an existing account, you'll likely be given the option to receive what are called E statements or paperless statements. This isn't just so that we can all do our part to minimize paper, this is also important because it ensures that sensitive information that's printed on paper isn't lost or stolen in the mail. Think about it, your monthly bank or credit card statements, have your full name, mailing address, portions of your account numbers, spending habits, locations of places you visit and total balance on them. That's a lot of information that makes it really easy for a criminal to know everything they need to know about you.

And since the information is usually in an envelope with a bank's logo and the information on it, it's usually pretty easy to identify. Going paperless ensures this sensitive information isn't just sitting around in a mailbox or on your doorstep for someone to simply pick up and walk away with. Instead, this

information will be sent to you via email. And if you choose to print a copy, you can. If you previously used paper statements or you choose to keep them, remember to always shred anything you are throwing away.

Yes. Tip number four is one of the most comprehensive measures you can take to ensuring a financial fraud doesn't grow out of control and it's to use a password manager. Coming up with a new password every time you need to create or update an account can be a headache. And to alleviate this, some people simply come up with one password that is unique to them that they can log into all of their accounts with. This is certainly easy to remember, but the problem is if someone gains access to one account, they essentially have access to every account where that password may be used. This is where password managers come in. They're third-party platforms that hold and generate strong passwords for you. This way, you don't have to think of a new one every time and you avoid duplication. Furthermore, if an incident of fraud does occur, you can easily identify and lock down the account that's affected.

Okay. The last tip on preventing fraud is using multifactor authorization. Multifactor authorization is the security measure that allows you to enable an additional layer of protection for a financial account. For example, for the first layer, you may be required to enter in your username and your password, but once you've done that, you may also be required to enter a code that's sent to the phone number or email address on file. This extra step can be a little time-consuming, but it ensures the person signing into the account is most likely the person who has rights to the account. Fraudsters are much more likely to move on to trying to access accounts that don't have additional layers of security them. So do yourself a favor and make it as difficult as possible for them to do it.