Financial accounting module 1 pdf

Want to learn about recording and collecting financial transactions? Want to look at the financial statements and understand the numbers you see? Start learning today with this Financial Accounting course where you will be wowed by comprehensive lessons taking you on a journey from double entry accounting right up to prepare and interpret a set of financial statements. Financial accounting is an important branch for the financial function of the company, without it the financial health and prospects of the company should not be determined. This course will go into business transaction and event logging, processing, reporting and aggregation. This course is especially beneficial if you want to: Equip yourself with the knowledge to take on the role of working as a junior within the Financial Accounting Department To start your own business and need an understanding of financial accounting Prepare an ACCA exam for financial accounting (FA) No prior knowledge required. Start learning today and speed up your business and finance sharp perceptions. To check availability of this course in your country, please click here. This course does not offer an edX certificate. Those students who want to earn a prize will be able to register for ACCA as a student, take computer based exams and obtain an ACCA diploma in accounting and business. You can find the nearest ACCA investigation centre on the ACCA website. Context and purpose of financial statements Qualitative characteristics of financial information use double entry and accounting systems How to record transactions and events How to prepare a trial balance sheet (including identifying and correcting errors) How to prepare basic financial statements for inline and unincorporated companies How to interpret and prepare simple consolidated financial statements Courses gave me confidence in my accounting knowledge. - Bree from the United States Studying with ACCA-X gave me confidence and knowledge. I got 95% in my FFA exam. And in less than one year, I was retrained and got the financial and management accounting job I wanted. - Vanessa Lavoipierre, from South Africa and UK Cybersecurity expert Paul Benda relays a story about the time hackers tried to break into his bank account and steal his money. They learned my login, but didn't know my password, says a senior vice president of risk and cybersecurity policy at the American Bankers Association.Fortunately, cyber thieves were foiled. I called my bank and locked down my account, Benda says. Such incidents could increase as hackers use american-accelerated embrace of mobile banks due to the coronavirus crisis. The FBI recently reported a 50 percent increase in mobile banking since the beginning of 2020, and warned that the increase would likely result in consumers inadvertently downloading fake banking apps and app-based banking Trojans designed to take ownership account information. These are not new threats consumers face, but a new theme has emerged, Benda says. Hackers are going after stimulus checks and Paycheck Protection Program (PPP) loans that Americans and small businesses have received from the federal government to survive the pandemic economic downturn. Tips to avoid getting hackedBankrate picked the brains of four cybersecurity experts to learn the best ways consumers can protect their bank and financial accounts. Here are their suggestions. From Paul Benda, senior vice president of risk and cybersecurity policy to the American Bankers Association: The number one way to protect yourself is to make sure you're really on your bank or financial institution's website or app when you're transacting a business – and not a fraudster site set up by hackers. Check your statement or back of your bank card right on the website, bookmark that, and use that, Benda says. Download verification apps only from reputable sites like the App Store or Google Play. Trojans are really devastating, says Benda. People need to be careful about what apps they install and where they install them. A high frequency of fraudulent activity can happen through so-called side-cover apps or those downloaded from unofficial sources, he adds. Pay attention to the privacy policy. Apps often say they need to drive photos, a microphone, and a camera. Banking apps will need access to these things, says Benda. People should make sure that they're happy with it. From Teresa Walsh, global intelligence officer at the Financial Services Information Exchange and Analysis Center, or FS-ISAC, the consortium focuses on reducing cyber risks in the global financial system: Stick to trusted app stores by downloading apps. Users should not download applications found in open forums, Walsh says. For banking applications, many banks offer links to app stores from their websites to ensure that you choose the right one. Beware of fraudsters receiving phishing emails while trying to get your personal information. Phishing emails often contain incorrect numbers or incorrect links. Don't answer them. Phishing awareness still refers to mobile threat mitigation because many people use their mobile emails and text messages from their banks, Walsh says. Not sure what kind of app experience to expect from your bank? Contact your bank to find out what features it has and how to access it safely. If you are confused at all, you should talk to your bank, Walsh says. From Donald Korinchak CyberExperts.com: If you want to avoid getting ripped off, don't make it easy for hackers to guess your PIN and password. The biggest problem with passwords is that people tend to reuse passwords and choose weak passwords, Korinchak says. This is because weak passwords are easier to remember. passwords are hard to remember, especially if you have dozens of different powerful passwords. But you will be better able to prevent cybercrime if you use longer passwords with a combination of uppercase and lowercase letters, numbers, and symbols. Use two-factor or multi-factor authentication to reduce the risk of exposure. This security measure requires you to provide at least two different factors to verify your identity. The additional layer of security required to access your account will provide more protection. There are three categories of authentication, Korinchak says. One, something you know like a password. Two, something you have like on your mobile phone – it's confirmed when you receive a text code. And three, something you are - biometrics. This latter example, such as fingerprint scan or iris scanning, is currently not widely used. Banks are starting to use biometrics by implementing voice printing technology during phone calls, he says. Set up alerts by email, text message, or financial institution app to monitor fraudulent activity. In the old days, customers were often unaware of the fraud until they got their monthly bank statements, he says. This delay could result in fraud for up to four weeks. Alerts are notified to the customer very quickly and can work with the bank to quickly correct the problem. Avoid sending financial or sensitive information via email because it is not encrypted and can be intercepted by hackers and used to raid your account. To protect your data, use the security features built into the device software. Be sure to create the ability to track your stolen device, unlock it and wipe it remotely, says Korinchak. Using strong passwords is easier if you use a reputable password manager or program that helps you generate, store, and manage personal passwords. Korinchak says password manager software is recommended by most cybersecurity experts. From Eric Kraus, Vice President of Fraud, Risk and Compliance Solutions to FIS, payment and financial technology solutions provider to merchants, banks, and capital markets around the world: In addition to downloading only verified apps from the App Store or the Google Play app store, run re-tested apps before downloading them. If a couple of consumers downloaded the app and had an abusive experience, they wrote about it in a review, says Krauss. Check your app's corporate email address. Does it look legitimate? If there is a strange spelling or email address looks off or if something doesn't look good, avoid it, he says. Like Norton or McAfee antivirus and malware tracking software helps protect your desktop computer, there are versions of mobile security software designed to protect your device and help you identify before you get tripped by hackers. The hint that something may be unthused is if you run the data faster than usual, or your battery is draining. This may indicate that something is quietly running in the background, says Krauss. to be involved in monitoring data and battery use. Avoid clicking on adware windows. It is a must way that fraudsters like to embed malware, Kraus says. Don't be too zealous clicking less than the scripully apps and ads that are pushed at you and popping up. Refrain from exchanging too much personal information on social media. Everyone wants to tell everyone in the world about every little personal thing in their lives, he says. Be aware of not oversharing. The more personal data a hacker has on yours, the more likely they are to use this information to find their way to your account. Consider using a reputable virtual private network or VPN on your computer to protect you from password sheaths. But avoid all that is free because they can't protect you at all. VPN can be very effective, says Kraus. They are not expensive and not difficult to build in your home. A bottom lineA study by the University of Maryland's Clark School of Engineering found that hackers attempt to attack computers with Internet access every 39 seconds on average. It puts responsibility on you to be vigilant of sinister tactics used by cyber thieves such as phishing and website spoofing designed to trick you into revealing confidential information. Hackers constantly improve their game, and it's up to us all to be vigilant, says Korinchak of CyberExperts.com.featured an image of 10,000 hours of Getty Images.Learn more: more: