POPPY BANK

Best Practices for Online Banking

Don't share passwords. The best way to keep accountability is to differentiate who has logged into the account online.

Create complex passwords which are a combination of numbers, letters and characters to make them harder to break. Do not use children's or pet's names or dates of birth.

Businesses, follow the practice of least privilege, allowing access to sub-users only as required to perform their job.

Use a bookmark to access the Bank's site. Avoid "direct navigation" which involves manually typing the Bank's address into a browser; a fat-fingered keystroke may send you to a look-alike phishing Web site or one that tries to foist malicious software.

For business accounts, consider taking advantage of Positive Pay. Any item that meets the criteria you establish will automatically post to your account. Your company will be notified via email of any rejected electronic item(s) that do not meet your filter criteria. Upon receipt of the rejected items, you can then return them or conveniently add filter criteria for future electronic transactions.

Close your browser after logging off of the Bank's online banking site.

Protect Your Business from Corporate Account Takeover

What is corporate account takeover?

Corporate account takeover is a type of fraud where thieves gain access to a business' finances to make unauthorized transactions, including transferring funds from the company, creating and adding new fake employees to payroll, and stealing sensitive customer information that may not be recoverable.

Corporate account takeover is a growing threat for small businesses. Cyber thieves target employees through phishing, phone calls, and even social networks. It is common for thieves to send emails posing as a bank, Delivery Company, court or the Better Business Bureau. Once the email is opened, malware is loaded on the computer which then records login credentials and passcodes and reports them back to the criminals.

How do I protect myself and my small business?

The best way to protect against corporate account takeover is to follow the security measures put in place with your financial institution. Work with your bank to understand security measures needed within the business and to establish safeguards on the accounts that can help the Bank identify and prevent unauthorized access to your funds.

Source Credit: ABA, Krebs on Security

A shared responsibility between the Bank and the business is the most effective way to prevent corporate account takeover. Consider these tips to ensure your business is well prepared:

Educate your employees.

You and your employees are the first line of defense against corporate account takeover. A strong security program paired with employee education about the warning signs, safe practices, and responses to a suspected takeover are essential to protecting your company and customers.

Protect your online environment.

It is important to protect your cyber environment just as you would your cash and physical location. Do not use unprotected internet connections. Encrypt sensitive data and keep updated virus protections on your computer. Use complex passwords and change them periodically.

Partner with your bank to prevent unauthorized transactions.

Talk to your banker about programs that safeguard you from unauthorized transactions. Positive Pay and other services offer call backs, device authentication, multi-person approval processes and batch limits help protect you from fraud.

Pay attention to suspicious activity and react quickly.

Look out for unexplained account or network activity, pop ups, and suspicious emails. If detected, immediately contact your financial institution, stop all online activity and remove any systems that may have been compromised. Keep records of what happened.

Understand your responsibilities and liabilities.

The account agreement with your bank will detail what commercially reasonable security measures are required in your business. It is critical that you understand and implement the security safeguards in the agreement. If you don't, you could be liable for losses resulting from a takeover. Talk to your banker if you have any questions about your responsibilities.

What Is Social Engineering?

Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software that will give them access to your passwords and bank information as well as giving them control over your computer.

Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak).

Source Credit: ABA, Krebs on Security

Security is all about knowing who and what to trust. Knowing when and when not to take a person at their word; when to trust that the person you are communicating with is indeed the person you think you are communicating with; when to trust that a website is or isn't legitimate; when to trust that the person on the phone is or isn't legitimate; when providing your information is or isn't a good idea.

Ask any security professional and they will tell you that the weakest link in the security chain is the human who accepts a person or scenario at face value.

Avoid opening attachments in emails you were not expecting. Be particularly wary of emails that warn of some dire consequence unless you take action immediately.

Remember that antivirus software is no substitute for common sense. A majority of today's cyber heists begin with malware that is spread via email attachments. Many of these threats will go undetected by antivirus tools in the first few days.

Avoid clicking links in emails that are unexpected or from an unknown source. Clicking a link could bring you to a website with malicious code that can then infect your computer. If you do receive a link that is unexpected from someone you know take the time to contact theme directly to confirm.

Never give personal information over the phone.

Mobile Banking Tips

Have a passcode on your mobile device, and lock it when not in use.

Choose a login ID that is at least 8 characters in length and includes letters, numbers and special characters.

Do not use your social security number as a login ID or PIN.

Do not use your mobile banking login ID and PIN for other online accounts.

Be cautious when entering your login ID and PIN in public.

Do not write down or share your login ID, password or answers to your security questions.

Always logout of your mobile banking web session or mobile banking app when you are done.

Keep your phone software and any app software as up-to-date as possible.

Delete your mobile banking text messages when you are done with your transactions.

Download mobile banking apps only from a trusted source.

Do not "jail break" or modify your mobile phone. This makes it much easier for hackers to download malware to your phone.

Source Credit: ABA, Krebs on Security

Avoid using public wireless hotspots to complete your online banking needs.

Monitor your bank accounts and statements on a regular basis. Receive alerts from online banking to monitor activity by setting up email notifications.

If you think someone has learned or stolen your login ID and password, notify Poppy Bank immediately.

Keep your phone in a safe location. If you lose your phone, notify Poppy Bank immediately.

Poppy Bank does not request personal information via telephone, email or pop-up boxes. If you receive suspicious telephone calls or email claiming to be from Poppy Bank, or if you have inadvertently given out your personal information, immediately contact Poppy Bank at (888) 636-9994 and the FBI's Internet Fraud Complaint Center at www.ic3.gov/default.aspx.

Source Credit: ABA, Krebs on Security