OUCH! November 2024

The Monthly Security Awareness Newsletter for You

# Don’t Let Cybercriminals Swipe Your Savings: Lock Down Your Financial Accounts!

## A Slick Scam and an Empty Bank Account

Emily was having a typical busy Tuesday. She grabbed her morning coffee, glanced at her phone, and noticed a text from her bank: “Did you make this transaction? Reply YES or NO.” She frowned. She hadn’t made any purchases yet that day. Maybe it was just a glitch.

She replied “NO,” and within minutes, a call came in. It was a woman claiming to be from her bank’s fraud department, speaking in a calm, professional tone. “We’ve detected unusual activity on your account. To secure it, we need to verify some details.” Emily, still groggy from sleep, complied. The caller walked Emily through a series of steps, asking for her online banking password and even guiding her to approve a notification on her phone. “This will block the hacker’s access,” the woman assured her. Emily followed along, not realizing she was falling into a trap.

Hours later, Emily’s phone buzzed again. This time it was a notification: $5,000 had been withdrawn from her savings account. Panicked, she logged into her bank app, but it was too late. The app wouldn’t accept her password. Her account was locked out. Then she saw another withdraw happen, and another.

In a flash, Emily understood. The “fraud department” call was a setup, a well-orchestrated attack by a cybercriminal who now had full control of her account. Emily quickly called her bank hoping she could save her bank account in time.

## Why You Need to Protect Your Financial Accounts

Our online financial accounts—checking, savings, and investment accounts—hold more than just money; they represent years of hard work, future plans, and financial stability. Cybercriminals are constantly on the lookout for opportunities to get access to your money, and one mistake can lead to significant financial loss. If you think a simple password is going to keep these criminals out, think again.

Today’s cybercriminals are smart, sneaky, and relentless. It's crucial to be proactive in securing your financial accounts. Not only will this help prevent unauthorized access, but it will also provide you peace of mind knowing that your hard-earned money is safe.

## Five Steps to Slam the Door on Cybercriminals

1. **Turn On Multi-Factor Authentication (MFA) Right Now:** Multi-Factor Authentication adds an extra layer of security to your online accounts by requiring you to verify your identity through two or more methods—something you know (password), something you have (smartphone or hardware token), or something you are (fingerprint or facial recognition). Even if a cybercriminal gains access to your password, they will still need the second factor to access your account. Always opt for MFA wherever available, especially for financial accounts.

2. **Use Strong, Unique Passwords:** Create strong, unique passwords for every account. The longer your password and the more characters it has, the better. One idea is to use a passphrase, that is a password made up of multiple words. Not a memory whiz? No problem. Use a password manager to help you generate and keep track of all of those long, unique passwords.

3. **Scams Are Constant—Don't Fall for Them:** One of the easiest ways for cyber attackers to gain access to your accounts is to ask you. They create emails, text messages, or even phone calls that look or sound like they are from your bank or financial institution. Always verify the source before clicking on links, downloading attachments or responding to messages or phone calls. The greater the sense of urgency, the more likely the email, message or phone call is an attack. The best way to protect yourself is go directly to your bank's official website by typing the address into your browser, or call your bank or financial institution back using a trusted phone number.

4. **Get Obsessed with Monitoring Your Accounts:** Make it a habit to frequently check your financial accounts for any unusual transactions. Even better, most financial institutions offer automated alerts for large withdrawals or suspicious activity. Setting up automated alerts can help you catch fraudulent transactions early and take swift action to minimize damage. If something doesn't look right, don't wait—take action right away.

5. **Keep Your Devices Locked Down Tight:** Your phone, laptop, and tablet are like vaults to your financial world. Keep them secure with a strong screen lock and the latest software updates, we recommend enabling automatic updating.

### Guest Editor

Elizabeth Rasnick is the Assistant Professor in the Center for Cybersecurity at the University of West Florida, with experience in programming and serving on an incident response team. She serves as the WiCyS Florida Affiliate senior vice president and holds a Doctorate in Information Technology.

### Resources

**Top Three Ways Cyber Attackers Target You:** https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
**Emotional Triggers – How Cyber Attackers Trick You:** https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/