141 eap

HELPING HANDS

# *Securing financial accounts*

(excerpts from "How to use automated alerts to protect yourself from fraud" Alliant Credit Union Newsletter, August 2018)

**Use smart passwords**

A key to reducing the risk that your accounts will be hacked is having strong, unique passwords for each account. How to create strong passwords in several reviews of breached login and password databases, security analysts found that the most common passwords were "123456" and "password." If you've created a password like that, with a single word or consecutive numbers, you are putting your accounts and finances in jeopardy. You take the same risk when you use a term that many people would associate with you, such as your first or last name, your phone number, your favorite hobby or team, or the name of your child or pet. Even if you know that password security is important, how do you create a password that is hard to hack yet easy to remember? Try using complex passwords created from phrases, words spelled backwards and a mix of letters, numbers and special characters.

**Make it easy for the bank to contact you**

Make sure the contact information on file for all of your financial accounts includes your email address and mobile phone number. Be sure to give permission to be contacted by phone, email, and text. That way, you can be contacted more quickly in case their fraud monitoring systems detect fraud on your account.

**Opt in to optional authentication steps**

If your financial institution offers any security measures in addition to a login and password, signing up for them adds a second hurdle for fraudsters to get over if they try to hack your account.

**Banking transaction alerts**

Monitoring your savings, checking and credit card accounts, which used to be time-consuming and a pain in the neck, is now a very simple and easy process. Just sign up for automated alerts that let you know whenever someone makes a transaction on your account. Signing up only takes a few minutes of your time, and after that, you're on autopilot. You'll receive an alert when there is a specific activity on your account.

- If you made the transaction, you ignore or delete the notification.
- If you didn't make the transaction, you contact your financial institution immediately to alert them to freeze your account before more fraud is committed.

**Customize your transaction alerts**

Many banks and credit unions that offer transaction alerts also allow you to customize the alerts so you can choose which transactions you want to be notified about.

Sign up to receive transaction alerts when your balance changes, when checks clear, when money is deposited or withdrawn from an account, or when your debit card is used.

- Opt in to receive account summary emails, stop-payment expiration notifications or NSF alerts when you have non-sufficient funds to cover a transaction.
- Set dollar limits for your alerts so only transactions over a specific amount will trigger a notification. This feature is especially useful for joint checking accounts. For example, you can set it up to only get alerts for transactions over $15 so you won't receive a

notification every time your partner spends $8 buying lunch with his or her debit card.

# Tips for Safe Online Shopping

(excerpts from Alliant Credit Union continued)

*Protect your computer*. Strong anti-virus software is a must. Anti-virus software protects your computer from viruses and can detect and remove them if they do make it onto your computer. Be sure to regularly install updates and run virus scans regularly to be sure there's nothing infecting your computer.

*Know who you're shopping with online*. A Google search brings up a host of well-known retailers, but other results are a little sketchy. If you've never heard of the retailer before, the deals seem too good to be true or the website is poor quality, be wary. It could be a scam site that's just after your personal information. Be careful about clicking on links to websites from emails, too. Scammers will often send phishing emails that appear to be from well-known retailers and include a link to a too-good-to-be-true offer. If you click on the link, it goes to a scam site or downloads malware onto your computer. Look for misspellings in the email, a tone that's not consistent with what you've received before or anything else out of the ordinary. Hover over the link before you click on it. If the URL doesn't match the URL of the retailer's website, it's probably a scam.

*Be sure you're shopping securely online.* Before you hand over your credit card information to a retailer, verify that the checkout is secure. A URL that begins with https:// means the site is using an SSL certificate, which secures all of your data as it passes from the website to the server and keeps it safe from hackers. To get an SSL certificate, a company must go through a validation process. There are different levels of security. The highest level is Extended Validation (EV), which means the company has proved not only its identity but also its legitimacy as a business. You know a site has an EV certificate if the search bar (or part of the search bar, depending on your browser) turns green and displays a lock icon.

# *IAM Peer Employee Assistance Program*

The heart and soul of the District 141 Employee Assistance Program is the local lodge EAP peer coordinator. These dedicated men and women volunteer their personal time to assist other union members and their families who are experiencing personal difficulties. EAP coordinators do not make clinical diagnoses or clinical evaluations, however, they are trained to make a basic assessment of your situation and refer you to an appropriate resource for a more detailed evaluation. EAP coordinators will follow up to ensure you have been able to access services that addressed the difficulty you were experiencing.

## IAM EAP Airline Chairmen

**United Airlines**
Kathy Ferguson: 703-505-4321,
E-mail: kf.borabora@cox.net

**American Airlines**
Chris Davis: 704-572-4859,
E-mail: chrisx1959@yahoo.com

**Hawaiian Airlines**
Meki Pei, mobile 808-208-5950,
E-mail: mekipei@gmail.com

## 2018 EAP Classes

William W. Winpisinger Education/Technology Center

EAP IV

September 16-21