CPS IBEW Federal Credit Union

FEBRUARY 2018

Watch Out for These Financial Scams

Financial scams are an increasingly consistent threat, so it's important to learn how to spot them. These threats come in the form of offers, deals, emotional pleas, and even intimidation, and they can find you anywhere – online, on the phone, and even on the road. The following are some of the most common scams to watch out for and how to outsmart them.

Online

"The internet has revolutionized our lives: You can do anything with a click of a button now," says CPS IBEW FCU President Adam Conine. "Unfortunately, that includes being scammed." Popular online scams include pop-up messages that warn about computer problems, online ads that offer amazing deals, fraudulent emails that ask for valuable personal information, electronic buyback offers, and even offers for Nintendo Switch emulators and other fraudulent computer or phone apps that, when installed, will steal your personal information.

According to Conine, it's OK to be skeptical. "Just as you wouldn't hand your wallet to a stranger on the street, you shouldn't give out your personal or financial information online with due diligence first," he advises. The FTC encourages consumers to research offers or claims online and with a consumer protection agency or the Attorney General's office before you make a purchase or agree to send money or to give or verify any personal information.

On the phone

Phone scams remain some of the most financially devastating events striking thousands of people each year. The most common scams to look out for right now include threatening calls claiming to be from the IRS, tech support calls claiming to be from Microsoft or Apple, and even calls claiming to be from loved ones or acquaintances in need of money (even billionaire Richard Branson was targeted with the latter

recently). Other calls that include offers for travel packages, credits or loans, high-stakes foreign lotteries, investment opportunities, extended warranties, trial offers and even some charitable causes are often scams.

The FTC advises—first and foremost—to resist any pressure to decide immediately and to keep your money, your financial information and your Social Security number to yourself. Any calls from the IRS are most likely scams (see the agency's guidance here) and so are unexpected phone calls from Microsoft or Apple tech support. Hang up and call these organizations yourself to confirm it was them. For other offers, follow the same advice for online scams and do your research.

Out on the road

Skimming devices on gas pumps and ATMs remain a problem because although businesses and consumers have started learning how to recognize these devices (which are connected to card readers or keypads to steal credit and debit card information), they are becoming more advanced and harder to spot. Red flags to looks out for include card readers or keypads that look different from those at the other pumps or ATMs, difficulty sliding the card or a loose or "jiggly" reader, or a broken or missing security seal (usually a red or brightly colored tape) placed over a fuel pump dispenser door. Some skimming devices can be placed inside a pump and so your only detection could be a missing or loose security tape.

"It's particularly important to be aware of skimming devices at gas stations and ATMs that are not monitored well," CPS IBEW FCU Chief Financial Officer Edna Narum explains. Non-bank ATMs account for the majority of compromised devices, reports FICO. Choose gas pumps and ATMs within sight of cashiers because they're more difficult to alter. For more information, click here to read "Gas Pump Skimming: Safety Tips to Protect Yourself."

How to "Freeze Card" With Our Home Banking and Mobile App

"Even the savviest people can fall victim to scams," Narum says. "It's important to spend just a few minutes each day monitoring your financial accounts so you can catch suspicious activity immediately."

For an added layer of security, Credit Union members can now freeze and unfreeze their debit cards through CPS IBEW FCUs Home Banking website. Freezing your card will give you a chance stop activity on your card while you investigate suspicious charges. Once logged in, you can find the "Freeze Card" button on the same screen as your transactions. While the card is frozen, call the 24-hour automated line at 1-866-842-5208 to report the issue so we can help you decide whether the card has been compromised. The card can be unfrozen by pressing "Unfreeze Card," which will appear in the same spot.

Members can also freeze and unfreeze debit cards using the CPS IBEW FCU mobile app. Simply log in to your account, select checking, then click the “Freeze Card” or “Unfreeze Card” option.

“We’ve made freezing your card so easy that I often advise members to get in the habit of freezing it whenever they aren’t using the card --while at work and when they go to bed at night, for instance,” adds Narum. “It only takes seconds and can give you valuable peace of mind.”

Image Copyright: opolja / 123RF Stock Photo