Apple Federal Credit Union Tips Help Consumers Avoid Email Scams this Holiday Season

FAIRFAX, Va. (December 3, 2018)—Cyber security specialists at Apple Federal Credit Union warn that the holiday season is prime time for criminals to be trolling the internet looking to steal your personal information. Phishing scams and fraud jump over 50% from the annual average from October through December, making the holiday season a dangerous time to be online. This data comes from a new report released by F5 Networks, Inc., a global company that specializes in application services and delivery networking, entitled 2018 Phishing and Fraud Report. To help protect personal data, including banking information, Apple Federal Credit Union has developed a list of tips to help consumers avoid cyber thieves.

"Phishing is a simple and common cyberattack because it works," says Larry Larsen, Director of Cyber Security at Apple Federal Credit Union. "You save the attacker a lot of time and inconvenience if you click on the link in his phishing email and enter your personal data. You just opened the door into a network without the bad guy having to decipher the passwords. People are busy and perhaps less vigilant—particularly given the volume of email advertisements and online transactions happening over the holiday season--so we always see a spike in this kind of cybercrime now."

Some common phishing attacks to beware of:

Account Verification—Many common social media and vendor sites (such as Facebook, Apple, Netflix, Amazon, or a financial institution) claim they are secure…and they are. But what happens when it appears that one of those sites sends a consumer an email telling him there is a problem with his account and he needs to login to fix it? The reality is that this is one of the most common personal phishing emails. Links within this will bring the target consumer to a fake website that looks legitimate and asks for his credentials. Logging in allows the attacker to steal personal information and use it for his own gain.

Fake Invoices--According to Symantec's 2018 Internet Security Threat Report, fake emails are the most common mechanism to deliver malware. Bad guys increase the chances that a target will open their email by claiming that an attachment is an unpaid invoice and that service will be cut off if it remains unpaid. This type of "spear phishing" email targets both individuals (by masquerading as Amazon, Apple and other such retailers) or businesses (by pretending to be one of their vendors or suppliers).

Package Delivery Email Notice—Many order holiday gifts online and watch for them to be dropped off at their doors. But anyone who receives a delivery notice for a package that he doesn't remember ordering beware, as this is a long-time phishing scam that garners significant results. An attacker will pretend to be FedEx, DHL or another mailing service and send the target a delivery notice with a link or attachment containing the details of the order. The attack commences when the target user clicks to

find out what's being sent to him and he is contaminated with malware or tricked into providing the attacker with his credentials.

Here are tips that consumers can use to avoid being scammed:

1. **Never click on hyperlinks in an email**. Consumers should always go to the site directly in their browser and find the page using internal links. If that is not possible, it's probably a scam. Or hover the mouse pointer over links to be sure they are real URLs before clicking them.
2. **Authenticate unexpected documents**. Unexpected documents received via email are a red flag. Pick up the phone, call the sender, and make sure it's valid before opening it.
3. **Test the legitimacy of suspicious emails**. Drag questionable emails with graphics or images into the Outlook "junk" folder. Email in this folder is stripped of the images, often leaving behind the URLs that can easily be scanned to see if they are genuine.
4. **Do not share personal data.** Do not give out personal details to anyone by way of email. If you determine the sender is legitimate, call them and give them the information over the phone. Regular email is not secure.

Keeping these tips in mind will help consumers to have a happier holiday.

About Apple Federal Credit Union

Established in 1956, Apple FCU is ranked as a top 100 credit union nationwide, serving nearly 210,000 members with $2.7 billion in assets. As a not-for-profit, member-owned financial cooperative, Apple FCU serves a diverse community of local education systems and anyone who lives or works in Fairfax, Frederick (VA) and Prince William counties. Members enjoy competitive rates, as well as fair and honest products and services, within a trusted environment. The Credit Union is fully committed to making a positive impact within the region, not only in financial services, but also in community involvement, financial literacy and charitable giving. To learn more, visit AppleFCU.org. Federally insured by NCUA. Equal Opportunity Lender.

# # #