DigiKnow

CYBER SECURITY DEPENDS ON YOU

Looking For A Pot of Gold? Watch Out For Tax Scams!

It's long been said, "Beware the Ides of March." This month we help you to be proactive when it comes to tax-related scams and begin a series of articles on securing the devices and apps we use everyday.

Protect Yourself From Tax Scams

Stay one step ahead of scammers this tax season by being proactive. Protect yourself with these steps:

- *File early* in the season so scammers have less time to steal your identity, file on your behalf, and collect your refund.
- Use the *strongest security settings* for your computer and update them whenever possible.
- Use *unique and strong passwords* for your banking and financial management accounts, credit or debit cards.
- Choose *two-step or multi-factor authentication* when conducting financial transactions online.

Remember, the IRS will never:

- *Call about taxes* owed without having first sent you a bill via USPS mail.
- Call to *demand immediate payment* over the phone or require you to use a specific payment method for your taxes.
- *Ask you to share sensitive information*, like a debit card number or checking account number, over the phone.

To report tax-related scams go to: https://www.irs.gov You should also report instances of IRS-related phishing attempts and fraud to the Treasury Inspector General for Tax Administration at **800-366-4484.**

Secure Your Router

Take some time to strengthen your digital age defenses against cyber attacks. Routers are chronically ignored by many consumers. *Consumer Reports'* data security and router experts say that taking the following steps can help protect you.

Turn On Automatic Updates

The easiest way to make sure your router always has the newest, safest software is to set up automatic updates, which are available on many models.

If your router doesn't allow automatic updates, you'll have to periodically download and install the new software from the manufacturer's website yourself.

Do this every quarter, advises Rich Fisco, who leads the router testing at *Consumer Reports*. "If you find your router is no longer getting updates," Fisco says, "it's too risky to keep using it. Verify its status with the manufacturer, and if it has reached the 'end of life' stage, buy a new router." Don't continue to use equipment that no longer has manufacturer support.

Use Strong Passwords

If you've never done so, you should *change two crucial passwords on your router:* the one that lets you manage the device's settings and the one that lets you connect other devices to its wireless network.

Install Antivirus Software

Antivirus software can protect your router—and by extension all devices connected to it—by identifying malicious software used to collect and encrypt the personal data on a computer, rendering it useless.

Visit the DTI Digiknow website for previous issues

eSecurity Newsletters

Questions, comments or topic suggestions?
Email us at eSecurity@delaware.gov

DEPARTMENT OF TECHNOLOGY & INFORMATION
DELIVERING TECHNOLOGY THAT INNOVATES

Delaware Department of Technology and Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links, or want to print a PDF copy, go to https://digiknow.dti.delaware.gov.