@DeldigiKNOW

DigiKnow
CYBER SECURITY DEPENDS ON YOU

February 2019

STUDENT LOANS AND SPEARPHISHING

The Cyber crime world is open 24/7, with new scams arriving every day. In this edition we look at Student Loan scams, and (not so) Happy Valentines Day messages, with a spear phishing hook.

FORBES' MAGAZINE'S TOP THREE SCAMS

Student Loan Consolidation Scam

The Scam: A student loan company will promise (for a fee) to consolidate your student loans and lower your monthly payments.

The Truth: The only official form of student loan consolidation is with the federal government. Check out Studentloans.gov or call 1-800-557-7394. There is no fee for student loan consolidation. If the company claims to have a relationship with the U.S. Department of Education, it's a scam.

IRS Student Tax Scam

The Scam: You receive a phone call from someone claiming to be an IRS agent who claims that you owe a "federal student loan tax." If you don't make immediate payment, the caller threatens arrest or a lawsuit from the IRS.

The Truth: There is no federal student loan tax. Importantly, the IRS always contacts you by mail first before calling you. They will never demand immediate payment, nor request a specific form of payment like a wire transfer or credit/gift card. They won't request personal or financial information by email.

Student Loan Forgiveness Scam

The Scam: A student loan debt company—usually through an online ad or email—will (for a fee) forgive your student loans.

The Truth: No student loan debt company will "forgive" your student loans—no matter how much you pay them. This scam tries to sound like Public Service Loan Forgiveness, which is a legitimate federal government program for public servants with federal student loans, but it's not.

Visit the DTI Digiknow website for previous issues.

eSecurity Newsletters

DON'T GET HOOKED!

It's nice to receive a Valentines Day greetings this time of year. Unfortunately sending and opening these greetings is like diving into a big pond of spearphishers.

Spear phishing is a pinpoint attack against some subset of people (users of a website or product, employees of a company, individuals) to attempt to garner information.

The most common scams are phony florists, malware laden electronic greetings, dating sites and fake delivery fees.

Don't trust online ads for florists and gifts unless you confirm that these sites are legitimate. Never give your credit card information until you are absolutely sure.

Be VERY wary of electronic greeting cards, especially those that read "from a secret admirer." Only open a card if you're certain it's from a person you know. Better yet, just don't open it.

Don't ever pay a "delivery fee" to anyone who claims that they need your credit card to cover the special fee for delivering alcohol, like a basket of wine.

Annual Information Security Training

The State network users' annual cyber security training is returning to a computer screen near you on February 4.

All employees with a Delaware.gov email address must complete this informative, interactive, self-paced cyber safety training each year. The training is available via the Delaware Learning Center, further information will be arriving in state email boxes.

Questions, comments or topic suggestions?
Email us at eSecurity@state.de.us

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.