K&K CONNECTIONS, LLC MONTHLY NEWSLETTER

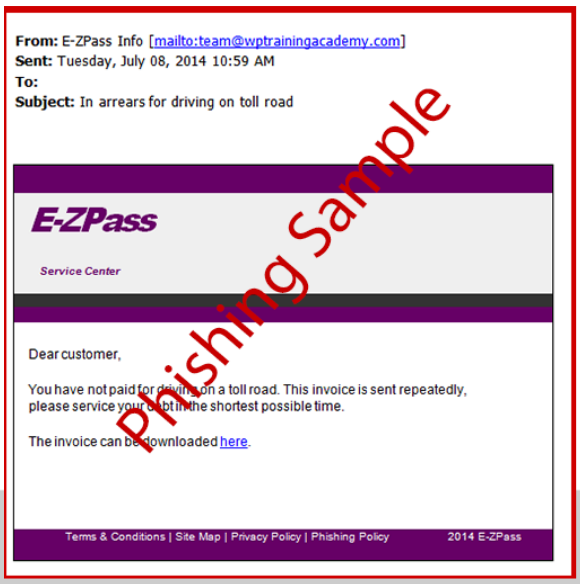
"ON THE MOVE"

"A Customer First Company"
July 2014

Welcome to the July 2014 Edition of "On the Move"

E-ZPass Phishing Scam

Recently, some E-ZPass customers have received the following email:



Customers are warned not to click on any emails that may seem suspicious. Also, it is important to take caution when downloading files on your computer. Here is a statement from the EZ-Pass website:

It was recently brought to our attention that many people have received a notice like the one below. Please be advised that this is not a communication from E-ZPass. It is likely a phishing scam. We advise you not to open or respond to the message. If you have questions about the validity of any message received from E-ZPass, please contact our Customer Service Center at 877-762-7824.
Valid emails originating from E-ZPass Virginia include the following return email addresses NoReply@ezpassva.com, customerservice@ezpassva.com and ezpass@ricklanddirect.com.

For more information visit
https://www.ezpassva.com/

Tips on How to Avoid Internet Scams

Every day, Americans receive offers, emails, pop-ups, and all sorts of information that must be sifted through in order to assess its validity. In the past, this information came primarily through the mail or by telephone. Now many of this information is now coming through the Internet. The on-line scams know no national borders; they respect no investigative jurisdictions, they are simply out to get you, your money, or personal information. Here are some tips you can use to avoid becoming a victim of internet scams:

- Do not respond to unsolicited e-mail.
- Do not click on links contained within an unsolicited e-mail.
- Be cautious of e-mail claiming to contain pictures in attached files; the files may contain viruses. Only open attachments from known senders. Scan the attachments for viruses if possible.
- Avoid filling out forms contained in e-mail messages that ask for personal information.
- Always compare the link in the e-mail to the link you are actually directed to and determine if they match and will lead you to a legitimate site.
- Log on directly to the official website for the business identified in the e-mail instead of "linking" to it from an unsolicited e-mail. If the e-mail appears to be from your bank, credit card issuer, or other company you deal with frequently, your statements or official correspondence from the business will provide the proper contact information.
- Contact the actual business that supposedly sent the e-mail to verify that the e-mail is genuine.
- If you are requested to act quickly or there is an emergency that requires your attention, it may be a scam.
- Remember if it looks too good to be true, it probably is.

For more information visit:
http://www.lookstoogoodtobetrue.com/

Information taken from www.fbi.gov and www.lookstoogoodtobetrue.com

K&K Connections, LLC Monthly Newsletter

"On the Move"

"A Customer First Company"
July 2014

How to Keep Your Personal Information Secure

There are four main ways you can keep your personal information secure:

1. Know who you share information with
2. Store and dispose of your personal information securely
3. Ask questions before deciding to share your information
4. Maintain appropriate security on your computers and electronic devices

The FTC has some important tips you can follow in all of these four areas.

- Lock your financial documents and records in a safe place at home, and lock your wallet or purse in a safe place at work.
- Shred receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, and similar documents when you don't need them any longer.
- Take outgoing mail to post office collection boxes or the post office. Promptly remove mail that arrives in your mailbox
- When you order new checks, don't have them mailed to your home, unless you have a secure mailbox with a lock.
- Make sure you know who is getting your personal or financial information. Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or know who you're dealing with.
- Before you dispose of a computer, get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive.
- Before you dispose of a mobile device, check your owner's manual for information on how to delete information permanently, and how to save or transfer information to a new device
- Use strong passwords with your laptop, credit, bank, and other accounts.
- Don't overshare on social networking sites. Never post your full name, Social Security number, address, phone number, or account numbers in publicly accessible sites.
- Be wise about Wi-Fi. Before you send information over your laptop or smartphone on a public network in a coffee shop, library, or other public place, see if your information will be protected.
- Keep financial information on your laptop only when necessary. Don't use an automatic login feature that saves your user name and password, and always log off when you're finished.

K&K Connection July Birthdays

We would like to wish everyone born in July a special HAPPY BIRTHDAY!

If we missed your birthday please let us know by emailing owilliams@ridek2k.com. Thank you!

Welcome To K&K Connections

We would like to say a BIG welcome to all of our new riders for the month of July. We are so very happy you have decided to join us!

Visit us at: www.ridek2k.com
Or Contact us at: info@ridek2k.com
PO Box 2010, Chester, VA 23831
Local: (804) 275-3872 Fax: (804) 275-3873