Commonwealth of Kentucky
Public Protection Cabinet

Matthew G. Bevin, Governor **David A. Dickerson, Secretary**

FOR IMMEDIATE RELEASE

Contact: Kelly May
502-782-9031 Direct
502-229-5068 Cell
kelly.may@ky.gov

Don't Fall for the Masquerade – Guard Against Phishing

DFI Offers Tips to Avoid Falling for an Imposter Over Email

FRANKFORT, Ky. (Oct. 25, 2016) – In financial fraud, the con artists may not be obvious – they may look like just about anyone, and they will do anything they can to gain your trust.

But in the online world, the cyber con artists have the ability to look like whoever they want – even masquerading as someone you know to trick you into falling for their attacks.

October is National Cyber Security Awareness Month. The Financial Cybercrime Task Force of Kentucky – a work group of the Department of Financial Institutions (DFI) – wants to take this opportunity to inform consumers about the dangers of phishing and spear phishing threats.

> ***Phishing*** is the attempt to obtain sensitive information (such as username, password, account details, etc.) or install malicious software by pretending to be a trustworthy entity in an email.
>
> ***Spoofing*** is when someone masquerades as another using false data (such as a forged email sender address, false Caller ID display number, etc.).
>
> ***Spear Phishing*** is a more targeted form of phishing that attempts to get your personal information with more sophisticated spoofing. Not only will it look like it's from a trustworthy entity, it may also appear to come from a specific individual you know, or it may mention information specific to you and your dealings with the entity.

"A DFI employee recently received a very real-looking email that appeared to be coming from a known person with an association we regularly deal with. The Commonwealth's Web Gateway and a policy of 'asking before acting' kept that spear phishing attempt from succeeding," said DFI Deputy Commissioner Brian Raley, who also is a Task Force member. "When using email, it's important for people to proceed with caution, even when things appear legit, and take some steps to protect their information."

DFI and its Task Force offer the following tips for Kentucky consumers to protect themselves from phishing attacks:

- Be suspicious, especially if the message appears to be "urgent" or requests you to "verify" personal or financial information. Common examples are messages claiming your password expired, your account has been suspended/locked or that there have been unauthorized transactions/account charges.
- Be cautious about opening attachments or downloading files from emails, regardless of who sent them to you. Ask yourself, "Was I expecting something from this person and do they normally send me

attachments/files in this manner?" If you are unsure, contact the sender directly to inquire about the email.
- Do not reply or click on links within the message. Hover over the link or email address to check out the actual destination. Retype web addresses directly into the browser window, rather than using the link. For emails, use "forward" rather than "reply" so that you are forced to type in the recipient's email address rather than use the email the sender provided.
- If you are concerned about your account, contact the business by telephone using a number you know to be genuine, not the number suggested in the email.
- Delete unwanted emails. Do not asked to be removed from unsolicited emails using the "opt out" feature. Your response only validates your email address, and further spam may follow.
- Ensure your browser is up to date and security patches are applied. Use anti-virus software and a firewall.
- Be wary of any message the urges you to act immediately or offers something that sounds too good to be true.
- Create strong passwords. Combine capital and lowercase letters with numbers and symbols into a password at least eight characters long to ensure that it's strong.
- Use different passwords for different accounts. That way if one account is breached, at least your other accounts should still be safe.
- Use strong authentication when available, especially for email and financial accounts. Take advantage of added security if your more sensitive accounts offer a layer of protection beyond just a password, such as a security question or a one-time PIN texted to a mobile device. Visit www.lockdownyourlogin.com for more information on strong authentication.

For additional information, review the DFI tip sheet and presentation, both called "Stopping Cybercrime – Tips for Consumers," available at http://kfi.ky.gov/public/Pages/scam.aspx.

What to know if you're a victim:
Reporting cybercrime to the appropriate authorities can help improve Internet safety and security for everyone. If you think you have been a victim of cybercrime or fraud, immediately file a complaint with your local authorities. Document the incident and the suspected source.

Complaints can be filed with the following federal government organizations:
- Phishing emails or websites – forward to US-CERT at phishing-report@us-cert.gov
- Online crime – Internet Crime Complaint Center (IC3) at www.ic3.gov
- Computer or network vulnerabilities – US-CERT at 888-282-0870 or www.us-cert.gov
- Fraud reports – Federal Trade Commission at www.ftc.gov/complaint
- Identity theft – www.IdentityTheft.gov
- Also, you might consider forwarding the phishing email to the bank, company or person it is attempting to impersonate.

For more information about National Cyber Security Awareness Month, visit the Department of Homeland Security at https://www.dhs.gov/national-cyber-security-awareness-month.

The Financial Cybercrime Task Force of Kentucky is a proactive, internal work group of DFI that focuses on best practice guidance and warnings for the financial services industry. The task force's goal is to identify and address emerging threats in cybercrime and security and to protect the integrity of Kentucky's financial system.

DFI, http://kfi.ky.gov, is an agency in the Public Protection Cabinet. For more than 100 years it has supervised the financial services industry by examining, chartering, licensing and registering various financial institutions, securities firms and professionals operating in Kentucky. DFI's mission is to serve Kentucky residents and protect their financial interests by maintaining a stable financial industry, continuing effective and efficient regulatory oversight, promoting consumer confidence, and encouraging economic opportunities.

###