IT Matters

Elizabethtown College Information & Technology Services Newsletter – March 28, 2017

Your Mailbox is Under Attack – Protect Yourself

It is crucial that you are cautious when reviewing, opening, and responding to email messages. Regardless of how effective mail filters are, they do not catch everything, and a phishing email might land in your inbox. To help you be prepared, we have compiled our most important phishing information into one handy newsletter for you.

Some things to note:

- E-town College & ITS will never ask for your password through email: never reply to an email with your password or personal information.
- Be skeptical when an email takes you to a log-in page. Double-check to ensure the log-in page is a valid page and not just a copy of the real thing.
- Confirm links before you click by hovering over links with your cursor. It will display the entire link, and you can ensure that everything is exactly how it should be, I.e. "etown.edu" not "e.town.edu.com".

Trust your intuition. If something doesn't feel right – **STOP**. Phishers rely on people making quick decisions and not thoroughly checking the message. If you're even a bit unsure, reach out to the Help Desk (717-361-3333 or helpdesk@etown.edu) to confirm the message before you click.

Don't Click, Hover

How do you know if a link is safe or not? Hover, don't click! When you hover over a link, it will tell you the full destination. Check to make sure that it links somewhere trustworthy. If not, don't click! It might be a scam or virus. If you think you might have received a phishing email, forward it to mailcop@etown.edu.

Hover »

Phishing Scams are Getting Smarter

Put your skills to the test. Can you spot the tell-tale signs of a phishing scam in this email? Give it a try. These phishing scams are getting smarter. Are you sure you can spot them all?

Catch the Phish »

Phishing, Smishing, and Vishing, Oh My!

Phishing is everywhere, so don't get hooked! These attacks can come over unprotected Wi-Fi networks, through unknown flash drives or SD cards, social media scams, and even through text (smishing) or phone calls (vishing). Use your common sense, and be wary of everything. Research before you click, even if it looks innocent.

Don't Get Hooked »

Never Reveal Your Password

It is very important that you know the difference between a real ITS email and a fake ITS email. This can help you spot a phishing email from a mile away. The real ITS will never ask for your password. Never enter your password into an unfamiliar or suspicious-looking webpage.

Protecting Passwords »

Gmail Email Scam

Phishing is a problem no matter what email you use. Keep an eye out for suspicious emails sent to all of your email addresses. Gmail has been the target of a few recent scams. Here's how to spot and report a common Gmail phishing scam.

Gmail Scam »

Connect With Us:

Facebook
Twitter
ITS Blog

Contact Us:

Phone: 717-361-3333
Email: helpdesk@etown.edu
Walk-in: Nicarry 125
Online Tickets: helpdesk.etown.edu
Website: www.etown.edu/its

Knowledgebase: Helpsheets and videos for 24/7 tech support
Atomic Learning: On-demand video tutorials on common technology topics