Alan Price

From: Alan Price
Sent: Saturday, April 11, 2020 4:19 PM
To: Staff_Official; Faculty_Official
Subject: Work From Home securely: take free, fast training and enter to win a Flying M gift card on us (IT Communication 10)

Good afternoon, and congratulations on making it through Week Two!
We know you've seen statistics about COVID-19, but have you seen anything about the simultaneous growth in cybercrime and threats? KnowBe4, a provider of cybersecurity training, reports a 667% (that's not a typo) increase in phishing attacks in March. Interpol, Europol, NATO, the FBI, and the Congressional Research Service all recently published articles and bulletins on COVID-19 related cybercrime and scams. Let's face it: most cybercriminals were already working from home when this started, so they're still going strong.

With most College employees now working from home this is an especially risky time for our information security responsibilities. We're planning to launch formal information security training this summer, but our partner, KnowBe4, made available a short, easy training course to help you prepare for and securely work from home. The first sections, about preparing for work from home, might be a bit late but can still help you optimize your home workspace. The later sections are excellent tips to make your workspace safe for your work and our data.

We ask that you take 15 minutes in the next week or two and try out this training. It applies to every employee and volunteer since educational records are protected by FERPA and the College is required to comply with various federal information laws.

To further incentivize you, we're offering the chance to win one of five $10 Flying M gift cards, donated by myself and Keith Bower, for completing the training and taking a very short survey about your experience and learning outcome. Winners will receive their gift cards when the College (and Flying M Caldwell…) reopen. You must complete the training and take the survey by May 1 to be entered to win.

The Training: https://goyot.es/kb4-wfhsec
The Survey: https://goyot.es/kb4-survey

Bonus Security Tip: you might have noticed that the above links are shortlinks, and you don't know where they go. Shortlinks are frequently used to hide malicious websites. In this case, goyot.es is entirely controlled by us and *generally* much safer than places like bit.ly or fb.me. However, you should still never completely trust a shortlink. When you click these links they'll take you to KnowBe4 and Microsoft Forms in Office 365. Make sure you're signing in to the real Office 365 by looking for the https://login.microsoftonline.com URL in your browser. Our logo only appears *after* you enter your YoteNet ID or when you were previously signed in.

If you have any questions after the training, or if you'd like to schedule a remote security check-up for your work computer, please contact us at helpdesk@collegeofidaho.edu

Stay safe. Stay healthy.

Sources:

https://www.knowbe4.com/coronavirus-security-awareness-resources
https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats
https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic
https://shape.nato.int/news-archive/2020/cyber-crime-amidst-of-covid19-threat-countering-malicious-activities
https://www.fbi.gov/coronavirus
https://crsreports.congress.gov/product/pdf/IN/IN11257