March 2020

LONGWOOD
UNIVERSITY
INFORMATION SECURITY

COVID-19 Scams

As you know, the Coronavirus, or COVID-19, is circulating worldwide. The Information Security Office wants to make you aware that you need to be vigilant about scams, emails, and malware that take advantage of the fear around this illness.

False COVID-19 Global Map

There is a false map circulating that claims to be from Johns Hopkins University and to show the global cases for COVID-19. Information Security has made this map inaccessible from Longwood servers, but if you are using a home computer you can still access it. It would be easy to come across it in a search for global incidences of the illness. Visiting the website infects the user's computer with an information stealing program which can take a variety of sensitive data.

Here are a few tips to help you determine if a website is fake:

- **Check connection security indicators.** A website that has an "https" tag is usually more secure—and therefore more trustworthy—than a site using the common "http" designation.
- **View certificate details by checking the site's security status in your browser's address bar.** For most browsers, a "safe" website will display a padlock icon to the left of the website's URL.
- **Pay close attention to the URL.** Even if you've verified that the connection is secure, be on the lookout for red flags like dashes and symbols in the names or domain names that imitate business names.

Continued on page 3...

Inside this issue

Special points of interest

- Securing the Human will soon be available for 2020
- Additional access may require additional training in Securing the Human; be prepared to finish new modules as they're assigned.

.

Avoiding Tax Fraud

As you know, tax season is upon us. US taxpayers are required to file their 2019 taxes by April 15. What you may not know is that you were able to file your taxes as early as January 27. To protect yourself against tax fraud, we recommend you file your taxes as soon as possible.

Remember this is the time of year when cybercriminals will try to scam you with tax-based attacks. Examples included cybercriminals calling you pretending they are the IRS and demanding you pay your taxes right away or they will arrest you. Or phishing emails explaining your taxes are overdue and you must go to a website or open an attachment to process your overdue taxes. Remember, any message that creates a strong sense of urgency is a big indicator of an attack. In addition, the IRS will never call or email you—the only way the IRS will reach out to you about any tax issues is by regular mail.

To learn more about tax fraud and additional ways to protect yourself, we suggest the articles File Your Taxes Before Scammers Do It For You and the IRS's website Taxpayer Guide to Identity Theft.

Remember this is the time of year when cybercriminals will try to scam you with tax-based attacks.

Did You Know?

- You can find information on data breaches on the FTC's website.
- The Identity Theft Resource Center tracks data breaches.
- You can learn more about the latest data breaches at Fraud.org.
- There is a long and interesting history of data breaches.

Handling a Data Breach

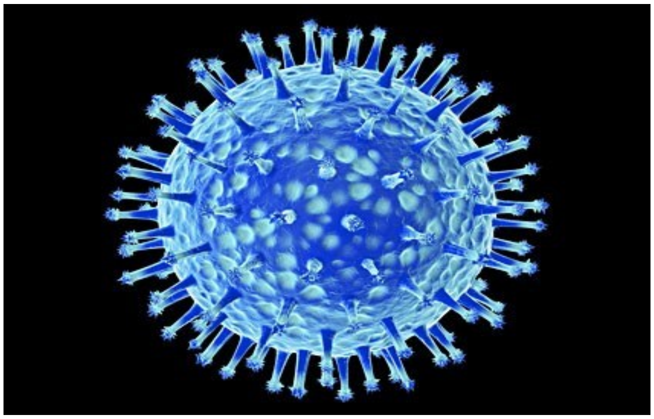
A data breach happens when your personal information is accessed or released without your permission, or is lost. Your breached information could be used to access your accounts, for identity theft, or to impersonate or blackmail you, causing emotional distress and financial loss.

If you're notified by an organization that your personal information has been breached, it's important to act quickly to reduce the impact on you. These notifications will let you know what personal information has been affected and what steps you can take.

If your data is breached, some steps you can take straight away are:

1. Change your passwords. Remember to use strong passwords that are different across each of your online accounts.
2. If available, turn on two-factor authentication as additional security to your passwords.
3. If your bank account has been affected, change your banking PIN number and monitor your bank transactions. If you spot any suspicious transactions, immediately report these to your bank.
4. Stay vigilant to scams. If your contact details were breached, a scam email might be personalized and address you by name.
5. Don't share your personal information until you are certain who you are sharing it with. If you're not sure, call the agency or organization back using publicly available contact details (such as from their website or a phone book).
6. If you have further questions about a data breach notification, contact the organization that sent you the notification.

From the article "What to do if your data is breached," on Stay Smart Online, the Australian government's online safety website.



COVID-19 Scams, Con't.

- **Watch out for invasive and aggressive advertising.**

Malicious Emails

The Cybersecurity and Infrastructure Security Agency (CISA) warns that cyber actors may send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes. **Exercise caution in handling any email with a COVID-19-related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to COVID-19.**

Here are some tips to ensure that you don't fall victim to an attack:

- **Be suspicious** of any phone call or message that:
    - **Pretends to be an official or government organization** urging you to take immediate action.
    - **Communicates a tremendous sense of urgency.** The bad guys are trying to rush you into making a mistake.
    - **Promotes miracle cures**, such as vaccines or medicine that will protect you. If it sounds too good to be true, it probably is.
- **Verify a charity's authenticity before making donations.** Review the Federal Trade Commission's page on Charity Scams for more information.
- **Avoid clicking** on links in unsolicited emails and be wary of email attachments.
- **Use trusted sources**—such as legitimate, government websites—for up-to-date, fact-based information about COVID-19.
- **Do not reveal** personal or financial information in email, and do not respond to email solicitations for this information.

For the latest updates visit the World Health Organization or the Center for Disease Control website. Please keep in mind these attacks can happen at work or at home, via email, text messaging or over the phone. Don't fall victim to bad guys playing on your emotions. If you feel you have received an attack at work, simply delete it or email phishing@longwood.edu if you have concerns.

Resources

- The World Health Organization (WHO)
- The Centers for Disease Control and Prevention (CDC)
- The Virginia Department of Health
- The Cybersecurity and Infrastructure Security Agency (CISA)

New Training Available

In the midst of the national and international focus on the coronavirus, many people are working from home. This is a time to focus on cybersecurity as well as physical security, as malicious actors are taking advantage of the situation to prey on the public, sending out malicious emails and creating malicious websites to trick users into downloading malware or giving away sensitive information. This is an excellent time for reviewing basic security practices.

With that in mind, the Information Security Office is launching the 2020 cycle of Securing the Human, our annual security training. Although this is a very busy time, taking the training now would serve as an important reminder to protect your information as well as the university's information.

We have updated the training this year, switching from animated videos to live action videos in which actors discuss important security topics. We have also shortened the training, as it had gotten too lengthy for most people to complete in one sitting. Please take the time to complete this important training as soon as possible, and be vigilant about your online activity.

The Office of Information Security is responsible for developing and implementing campus-wide policies, controls and procedures to protect the university's information technology resources and systems from intentional or inadvertent modification, disclosure or destruction, as well as monitoring user adherence to these policies.

Longwood University

Information Technology Services
French Hall
201 High Street
Farmville, VA 23909
(434) 395-4357
(434) 395-2034

Fax: (434) 395-2035