March 2019

LONGWOOD UNIVERSITY

INFORMATION SECURITY

Identity Theft

Identity theft has become a fact of life during the past decade. If you are reading this, it is a safe bet that your data has been breached in at least one incident. Does that mean we are all helpless? Thankfully, no. There is a lot we can do to protect ourselves from identity theft and to make recovery from cyber incidents quicker and less painful.

First, take control of your credit reports. Examine your own report at each of the "big three" bureaus. You get one free report from each credit bureau once per year. You can request them by going to AnnualCreditReport.com. Make sure there's nothing inaccurate in those reports, and file for correction if needed. Then initiate a credit freeze at each of those plus two other smaller ones. Instructions can be found at Krebs on Security. To keep an eye on your credit report all year, space out your credit bureau requests by requesting a report from a different credit bureau every four months.

Next, practice good digital hygiene. Just as you lock your front door when you leave home and your car when you park it, make sure your digital world is secured. This means:

1. **Keep your operating system up to date.** When OS updates are released, they fix errors in the code that could let the bad guys in.
2. **Do the same for the application software you use.** Web browsers, plug-ins, email clients, office software, antivirus/antimalware, and every other type of software has flaws. When those flaws are fixed, you are in a race to install that fix before someone uses the flaw against you. The vast majority of hacks leverage vulnerabilities that have a fix already available.

Continued on page 2

Inside this issue

Special points of interest

- The first full week of March is National Consumer Protection Week.
- “Directory Information” has changed at Longwood. See “Finding Ferpa” on p. 2.

Two-Factor Authentication

Two-factor authentication, also known as two-step verification, is coming to Longwood. Two-factor authentication is an extra layer of security to ensure that you are the only person who can access your account, even if someone else knows your password.

To use two-factor authentication, you will need your LancerNet ID and password and a device. The device can be a Smartphone, tablet, or a hardware token. After logging in to a Longwood system with your LancerNet ID and password, you'll be prompted to confirm your identity a second time using the device that has been attached to your account.

We have already begun using two-factor authentication on the VPN, or Virtual Private Network. Information regarding what systems will utilize two-factor authentication and a timeline will be communicated as it becomes available.

"Some of those fun-to-share-with-your-friends quizzes and games ask questions that have a disturbing similarity to 'security questions' …"

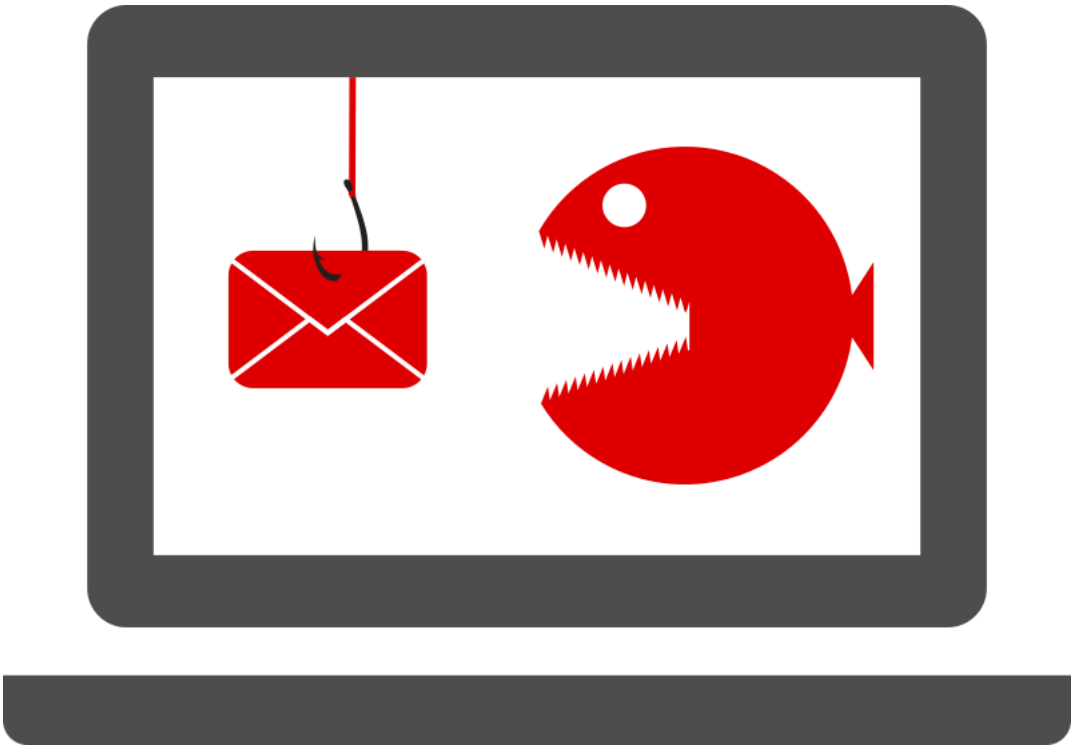
Reclaim Your Identity

If you've been a victim of identity theft:

- Create an Identity Theft Report by filing a complaint with the **Federal Trade Commission** online (or call 1-877-438-4338).
- Use the Identity Theft Report to file a police report. Make sure you keep a copy of the police report in a safe place.
- Flag your credit reports by contacting the fraud departments of any one of the three major credit bureaus: **Equifax** (800-685-1111); **TransUnion** (888-909-8872); or **Experian** (888-397

Identity Theft, Continued

3. **Engage your brain.** Think before you click. Think before you disclose personal information in a web form or over the phone.
4. **Think before you share on social media sites.** Some of those fun-to-share-with-your-friends quizzes and games ask questions that have a disturbing similarity to "security questions" that can be used to recover your account. Do you want the answers to your security questions to be published to the world?
5. **Use a password manager** and keep a strong, unique password for every site or service you use. That way a breach on one site won't open you up to fraud at other sites.
6. **Back. It. Up.** What do you do if you are hit with a ransomware attack? (Or a run-of-the-mill disk failure?) If you have a recent off-line backup, your data are safe, and you can recover without even thinking about paying a ransom.
7. **Full disk encryption is your friend.** If your device is stolen, it will be a lot harder for a thief to access your data, which means you can sleep at night.
8. **Check all your accounts statements regularly.** Paperless statements are convenient in the digital age. But it is easy to forget to check infrequently used accounts such as a health savings account. Make a recurring calendar reminder to check every account for activity that you don't recognize.
9. **Manage those old-style paper statements.** Don't just throw them in the trash or the recycle bin. Shred them with a cross-cut shredder. Or burn them. Or do both. Data stolen from a dumpster are just as useful as data stolen from a website.



What to Report

You may have wondered why the Information Security Office is asking you to forward certain emails to us and not others. Certain email categories represent a potential threat to Longwood University in the form of compromised credentials or information. Other categories of email carry no threat to Longwood but instead threaten your wallet.

- **Phishing emails** represent a very real threat to Longwood, and Information Security needs your help to thwart these nefarious attempts to gain unauthorized access.
- **A phishing email** will attempt to get the recipient to pass along credentials (username and password) that would allow the attacker to access Longwood systems.
- These emails can have the credential request in the body of the email or will attempt to redirect you via a link or attachment to a site to enter logon credentials.
- **Please report these to phishing@longwood.edu** as we will use this information to warn the campus about the phishing attempt, and to implement prevention measures if needed.

- **Spam emails** do not represent a threat to Longwood University but they can be annoying and confusing.
- These emails typically are trying to get money from you in some form and can include links to sites with ads or popups or other undesirable detritus.

Finding FERPA

Are you familiar with FERPA guidelines? Do you know where to find information about it?

FERPA, or the Family Educational Rights and Privacy Act of 1974, is a federal law that protects the privacy of student education records and requires the establishment of policies to safeguard student records and data. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education; Longwood student records policies comply fully with FERPA.

You can find Longwood's FERPA policy at: http://solomon.longwood.edu/registrar/policies--procedures/ferpa.php

Recently, Virginia has ruled that a student's email address does not count as "directory information," and therefore cannot be shared. Although FERPA allows the sharing of student email addresses, Longwood no longer does so.

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.

What to Report, Continued

- Many of these emails are scams, and they begin to circulate widely. If you are concerned about the rest of campus receiving the email, you can send it to infosec@longwood.edu. We will use this information to warn the campus about the scam.
- Individual spam emails do not need to be reported. The best way to deal with them is to right click on the email and click Junk > Block Sender. You can also contact the Help Desk at (434) 395-4357 for additional assistance.

Email attachments and links can be questionable. While Information Security can guide you in regards to email attachments, we cannot make the decision to open or not to open. If you have an attachment that you have any questions about, please visit our phishing indicators page: http://solomon.longwood.edu/information-security/security-alerts--information/phishing-indicators/

Longwood University

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

Fax: (434) 395-2035