ISSUE: September YEAR: 2021

Security Awareness Newsletter

Preparing people to lead extraordinary lives

For every lock, there is someone out there trying to pick it or break in.— David Bernstein

The Hybrid Workplace

The Human Element

If you ask any cybersecurity professional what the weakest link in the corporate security chain is, they will tell you that it is the employee. This can be seen through the phishing campaigns that have been used to lure users in and attempted to steal their data. In April 2020, Google claimed to be blocking over *240 million* COVID-themed spam messages each day, and *18 million malware* and phishing emails.

Remote employees are more exposed than ever because they may be distracted by housemates or family members, and therefore more likely to mistakenly click on malicious links. Contacting IT support or even getting a colleague to sanity-check a suspicious email is much harder when working remotely, while personal laptops and home networks may also offer fewer protections from malware.

Now that workers are returning to the office, there are understandable concerns that they may bring bad habits learned over the past 18 months with them.

Challenges of the Cloud

The pandemic has also exposed the remote working infrastructure. For example, think about the exploits targeting unpatched VPNs and misconfigured RDP servers protected with weak or previously breached credentials. ESET reported that there was an increase of 140% in RDP attacks in the third quarter of 2020.

The adoption of new cloud services also drew the attention of an increase in threats last year. There are persistent concerns over vulnerabilities, as well as reports of stolen account passwords and anxiety over security and privacy of an organization.

A hybrid workplace will arguably require even more shuttling of data between remote workers, cloud servers and office-bound employees. This calls for employees needing to be safer when it comes to cybersecurity.

A More Secure Workplace

There are many things that an organization can do to be more secure. From having access restricted according to least privilege principles, to having network segmentation put into place to further limit potential malicious activities, the workplace will be in much better shape to deal with cyber threats. Please see below for some of the cybersecurity foundations that will help keep an organization more secure:

Security Awareness, Training, and Education

It is important to have ongoing security awareness training, as well as live simulation exercises that develop muscle memory or instinctive behavior for employees to recognize, foil and report social engineering attempts.

Awareness can also be brought to individuals by incorporating visual guidance or inconspicuous cues and nudges to gently guide employees in making sound security decisions.

Strong and Secure Passwords

Use passwords on all your devices and applications. Make sure the passwords are long, strong, and unique: at least 12 characters that are a mix of numbers, symbols, and capital and lower-case letters.

It is also recommend to add a password screen every time you access your laptop and other devices so that if your device is breached or falls into the wrong hands, it will be harder for a third-party to access your sensitive files. Using a password manager tool to help keep all your passwords secure is also good practice.

Source: We Live Security, Security Magazine

Back-to-School Cybersecurity Tips

Beginning of the Year Scams to Look Out For

Please be aware of the information below to look out for when it comes to cybersecurity tips to stay safe:

- Emails supposedly containing "important information about your LUC account," or a "problem with your registration"
- Scams specifically designed to cheat students out of money, such as scholarship scams, fake "tuition payment processors", textbook rental or book-buying scams, housing scams, tutoring scams, and work-from-home scams
- "Tech support" scams where you get a call supposedly from "the Service Desk" or even "Microsoft" or "Apple" telling you there's a problem with your computer
- IRS impersonators demanding that students or their parents wire money immediately to pay a fake "federal student tax"
- Messages asking for your login information, no matter how legitimate they may look. No one other than you need to know your passwords
- Fake friend requests on social media
- Fake Box or Google Doc notices

How to Stay Safe

The best way to avoid scams is to approach all unexpected messages, offers, and phone calls with healthy skepticism. Helpful habits include:

- Always think twice before clicking on links or opening attachments, even if they look like they're from someone you know. If you're not sure, contact the sender by a method you know is legitimate to confirm they sent it.
- Verify requests for private information. Remember, con artists know how to fake their identity.
- Protect your passwords. Make them long and strong, never reveal them to anyone, and use different passwords for different accounts. Also, use multi-factor authentication (MFA) where possible.

Source: UC Berkley

Top 3 Coronavirus Phishing Scams

1. Consumer Relief Package: As the economic fallout of the COVID-19 pandemic continues, attackers are leveraging consumer anticipation of tax relief and government issued economic stimulus plans. These attacks trick victims into dropping their guard and clicking malicious links.

2. Help Desk Impersonation: At a time when technical support teams are helping employees transition to remote workstations, cybercriminals are impersonating IT help desks to take advantage of their increased visibility and communication.

3. Internal Organization Alert: This phishing attack takes a corporate approach by impersonating a company's president to deliver an attachment disguised as tips to prevent infection. The attachment is designed to infect employee's machine with malware.

Source:

University Information Security Office
LUC.edu/its/uiso/

ITS Service Desk
Email: ITSservicedesk@luc.edu
Telephone: (773) 508-4487
Hours: LUC.edu/its/service/support_hours.shtml