Cybersecurity Awareness for E-Learning

E-learning is an important tool to help us teach and learn while staying safe. However, cyber safety is an important aspect of digital learning. Please follow the following e-learning cybersecurity guidelines to keep yourself and your fellow teachers, students and school safe.

Choose Strong Passwords

Your passwords for your email and any school applications need to be strong – and they shouldn't match each other.

> According to a study conducted by Microsoft, 44 million email accounts worldwide were vulnerable to cyber threats because of weak passwords in 2019 . Not only do weak passwords open up your school system to cyber threats, but hackers can also use this information to gain access to your personal accounts as well[1].

A strong password should have:

- At least 8 characters.
- A mixture of upper and lowercase letters.
- At least one number.
- At least one special character.

Your passwords for your school accounts should be different from your personal accounts.

Beware of Phishing Attacks

> Phishing and email attacks are the leading cause of information breaches in the world. 92% of all malware is delivered through email, 30% of phishing attempts are successful, and the volume of email fraud is increasing by 8% year-over-year[2].

[1] https://securityboulevard.com/2020/04/8-scary-statistics-about-the-password-reuse-problem/#:~:text=Microsoft%20recently%20announced%20that%20a,as%20many%20as%2014%20times.
[2] https://purplesec.us/resources/cyber-security-statistics/

Phishing attacks are hacking attempts that come through disguised as a friendly communication – often an email. In a phishing attack, hackers attempt to draw out your personally identifiable information by pretending to be figures of authority, embedding malware in links, and attaching harmful documents.

To keep your inbox safe from potential hackers, follow these steps:

- Be wary of every email you receive. If it looks suspicious, don't open it. Common red flags include:
  - Poor spelling or grammar.
  - A request for confidential information.
  - A sense of urgency.
  - A sender email that doesn't match the sender's name.
  - Embedded links that seem strange or suspicious.
- Do not click on any links or open any attachments unless you're positive the sender is legitimate.
- Don't enter your personal information (name, address, SSN, etc.) in a pop-up screen.
- Keep your email passwords unique - don't recycle the same passwords for other applications.

Keep Social Media off School Devices

Any devices provided by the school should be used for school-related work only. Phishing scams can take place outside of email, and hackers often target social media apps like Facebook or WhatsApp for their hunting grounds. Hackers will use these social media platforms to obtain access to your device, implant malware, and viruses, or access your personal

> In fact, according to a recent study, 83% of phishing attacks targeted social media apps, messaging apps, gaming apps and other non-email locations[3].

To keep yourself and your school secure, any personal work or online leisure activities should be kept to your personal devices.

BridgeTek Solutions

At BridgeTek, we specialize in the education industry. We understand the unique nuances of the education community, which allows us to design solutions to meet your industry-specific needs.

Let us help you navigate the world of e-learning security.

Contact us today

www.bridgeteksolutions.com
(864) 214-0221

BRIDGETEK SOLUTIONS

CISCO Partner
Premier Certified

[3] https://keap.com/business-success-blog/business-management/human-resources/security-challent=In%20a%20landscape%20like%