Schoolzine Email Policy 2020

OVERVIEW:

Email is Schoolzine's most prominent form of communication as it provides many benefits. However, misuse of email can post many legal, privacy and security risks, thus it is important for users to understand the appropriate use of email and remain vigilant.

Email security

Email is often the preferred method of phishing attacks, confidentiality breaches, viruses and other malware. These issues can compromise our reputation and our equipment.

Ensuring you comply with the following will reduce your risk:

- Select strong passwords with at least eight characters (capital and lower-case letters, symbols and numbers)
- Do not open attachments that you were not expecting to receive
- Be suspicious of clickbait and generic subject lines (eg: *Remittance Attached*)
- Check the email address and name of senders to ensure they are legitimate (*Pay attention to misspelled domains. Eg: admin@facebok.com*)

These few reminders can help you spot a phishing email:

1. **Legitimate companies don't request your sensitive information via email**
2. **Legitimate companies usually call you by your name** (*They don't begin emails with "Hi Dear," or "Hello @schoolzine.com,"*)
3. **Legitimate companies have domain emails** (*Their email addresses include their company name, eg: luke@schoolzine.com seems valid, luke.schoolzine@y7mail.com does not)*
4. **Legitimate companies know how to spell and use grammar**
5. **Legitimate companies don't send unsolicited attachments** (*Be especially vigilant with, .doc .txt .bat or .exe files*)

6. **Legitimate company links match legitimate URLs** (*You can see where a hyperlink is pointing by hovering over it. Look at the URL and make sure it matches what you are expecting*)
7. **If it sounds too good to be true, it probably is** (Surely we can't ALL have won the Irish lottery!? I didn't even know I bought a ticket.)

If an employee isn't sure that an email they received is safe, they should contact the Support Team. **If you suspect that you have downloaded an unsafe file or clicked on a malicious link please notify the Support Team immediately**.

Machines that are suspected of being compromised will need to be **removed from the network as soon as possible** and reviewed by Support. A singular infected machine, connected to our network, could potentially infect mail servers, local drives (D, T, S etc), and if serious enough, SZ+ as a whole.

We remind our employees to keep their anti-malware programs updated.

Inappropriate use of company email

Employees represent our company whenever they use their corporate email address. They must not:

- Sign up for illegal, unreliable, disreputable or suspect websites and services.
- Send insulting or discriminatory messages and content.
- Intentionally spam other people's emails, including their coworkers.

Resources:

- Prevention tips from Google: https://www.youtube.com/watch?v=R12_y2BhKbE
- Phishing explanation: https://youtu.be/Y7zNlEMDmI4
- Example Phishing emails: https://www.phishing.org/phishing-examples