Ceres Unified School District

Cybersecurity Guide

Most cyber threats will target <u>human beings</u> as their primary means of attack. The information below highlights the most common methods a cyber criminal will use.

Phishing

What is it? - Phishing attacks occur when an email is sent to people within an organization pretending to be someone or something they know or trust such as an online bank, government entity, or even a co-worker. The phishing email will usually contain a request, sometimes threatening, asking for you to open an attachment, click a link, or reply with your username and password or personal information.

How can I identify a phishing email?

1. Do you know the sender of the email, and can you recognize their email address? Were you expecting to receive the email? If not, report it or delete it.
2. Is the email requesting you to open an attachment, click on a link, or share sensitive information? Does the message seem threatening? If so, please report it or delete it.

What will it do? - If a link or attachment is opened within a phishing email, it infect your account(s) or computer(s) in the following ways.

1. Install malicious software such as a virus, ransomware, or a keylogger.
2. Hijack your organization's network to steal bandwidth using a bot
3. Hijack your organization's storage infrastructure to store illicit content.
4. Hijack highly sensitive personal information to distribute online or sell.

What should you do if you receive a phishing email? - Please do not open or click on any items that are part of the email, and do not reply to the email. It should be reported to the Technology Services Help Desk at https://helpdesk.ceres.k12.ca.us or helpdesk@ceres.k12.ca.us

Social Engineering

What is it? - Cyber criminals will often use various forms of social engineering to pretend to be someone or something they are not. It is a form of psychological manipulation that tricks the target into believing the attacker.

How can I identify it? - An attacker will use various techniques that "con" you into doing what they say. They will often pretend that they are trying to be helpful (fraudulent credit protection service asking for your information) or scare you into thinking something there is an urgent problem (tricking you into thinking your computer has a virus). Often times, they will call you over the phone, use indiscriminate social media accounts, or email (phishing).

What should you do? - Look or listen carefully to the message that is being shared with you. If it does not seem valid or is too good to be true, it could be a scam. For example, if you receive a call stating that your computer has a virus, it is likely coming from a fraudulent source. Think about the message. Have you or others ever received a call like that before? Another example would be an attacker stating that your credit card has been compromised. Check the validity of this statement by hanging up or deleting the email and contact your credit card company.

Best Practices

Passwords - Use a passphrase of 8 characters or more to create a strong password. Never share your password or type it into an online form. Never create weak passwords (Password123) or reuse passwords across different sites or systems.
Data Security - Do not gather and maintain unnecessary data. Do not leave sensitive data on devices (laptops) or storage platforms (USB drives) that are portable as these can be easily lost or stolen.
Records Security - Always ensure records are secured either in a file cabinet (physical records) or on a password protected account or folder provided by the district that only you have access to (digital records).
Applications, Programs, and Software - Always download applications, programs, and software from a reputable vendor and host. There are many variations of counterfeit services and software available on the web. Be on the look-out for software that does not have a company name tied to it.
Report - Any suspicious digital activity should be reported to the Technology Services Help Desk at https://helpdesk.ceres.k12.ca.us or helpdesk@ceres.k12.ca.us