Bits & Bytes Online Newsletter

• Bi-weekly online newsletter used to strengthen user awareness of current cybersecurity threats and vulnerabilities – each article takes only 3 to 5 minutes to read.
• Includes best practices users can take at work and at home to reduce risk.
• Links to additional information available on other government sites are provided to enhance learning.
• Includes catchy titles and colorful graphics to draw the user’s attention.
• Reinforces incident reporting requirements and provide instructions on how to report known or suspected cybersecurity incidents and phishing attacks.
• A link to each newsletter is included in a Department-wide communications announcement emailed to all users, ED Notebook, with the newsletter available on the Department’s Intranet.
• The newsletter title makes it an easy to remember resource and the online format increases overall impact as users may use the newsletter as a job aid or include the information and tips in Principal Office level communications.
Each article describes the threat or vulnerability in terms easily understood by all users.

Department requirements as well as tips and best practices to protect the user at work and at home are included.

Reduces risk by increasing awareness.

Cybersecurity Bits & Bytes: Passwords Under Attack

What are password attacks?
A password attack simply refers to your password being stolen by a hacker, although there are a variety of ways that threat actors can obtain this information. Over the years, password attacks have evolved and are now responsible for 81% of data breaches. Some of the most popular types of password cyber-attacks are:

- Brute-Force Attack: In a brute-force attack, hackers make numerous hit-or-miss attempts, usually using automated methods that try multiple letter-number combinations. A hacker can try 2.18 trillion username/password combinations in 2.2 seconds, and if your password is simple, your account won’t stand much of a chance against this type of attack.
- Keylogger Attack: A keylogger is a spyware that records a user’s activity by logging keyboard strokes. Threat actors use keyloggers to record not only the username and password but also the website or app where those credentials were used.
- Dictionary Attack: Dictionary attacks are a type of brute-force attack based on a list of commonly used words and phrases, as well as often-used passwords. These words are not actually limited to words in the dictionary and can include things like popular pet names, movie characters, and people.
- Credential Stuffing: Like brute-force attacks, credential stuffing uses trial-and-error to gain access. However, instead of guessing passwords, attackers use stolen credentials as credential stuffing works on the assumption that people tend to reuse passwords for multiple accounts and across various platforms.
- Copying/Shoulder Surfing: Of course, we can’t overlook the old-fashioned password-stealing options of simply copying down a password that is found physically written down somewhere or watching over someone’s shoulder and observing their credentials as they enter them.

What can I do to protect against password attacks?
The best way to prevent password attacks is to adopt password hygiene and management best practices. Boosting password security significantly improves your ability to avoid a data breach. In accordance with the Department of Education’s Standard PR.AC Password Parameters, the mandatory standard for accessing ED information systems is via two-factor identification, using both a Personal Identity Verification (PIV) card and a Personal Identification Number (PIN). System access using only a password without a PIV card is only permitted if PIV usage is not a technically viable option such as on legacy systems that lack PIV capability. A PIV exemption risk acceptance form must be submitted to Information Assurance Services (IAS) for approval. Review the Standard PR.AC Password Parameters for specific requirements and consider these best practices for creating and maintaining strong passwords:

- Avoiding passwords based on personal information: This includes data like your name and date of birth.
- Avoid dictionary words: Dictionary words make you more vulnerable to dictionary attacks.
- Modifying easy-to-remember phrases: One way to do this is to think of a passphrase, like a line from a song, then use the first letter from each word, substituting numbers for some of the letters.
- Using the most complex password a platform will allow: Whether a platform allows 8, 12, or more maximum characters, use them all. The more complex your password is, the harder it will be to crack.
- Using unique passwords for each platform: Reusing passwords across platforms opens you up to having all your data stolen once a single password is compromised.
Concise “bite-sized” learning

At the end of each article, links to additional information available on other government sites are provided to enhance learning.

For more technical threats or vulnerabilities, information is provided to help the user better understand the risk.

Cybersecurity Bits & Bytes: Zero-Day Attacks

What are zero-day attacks?
The term “zero-day” refers to a software vulnerability before developers are aware of it. With these vulnerabilities, there have been zero days for software makers to develop and release a patch. There are three important terms when it comes to these kinds of attacks:

- Zero-day vulnerability—a flaw in security software that’s unknown to the developer
- Zero-day exploit—a zero-day vulnerability used for malicious reasons by threat actors
- Zero-day attack—a cyberattack leveraging a zero-day exploit, often resulting in identity theft or data loss

To put these zero-day definitions together, zero-day vulnerabilities leave us susceptible to zero-day exploits, which are manipulated to carry out zero-day attacks.

What’s the risk?
Record-high numbers of zero-day exploits were tracked in 2021—double the number found in 2020. But why is this significant? Zero-day exploits are difficult to defend against because data about the exploit is generally only available for analysis after the attack has happened.

How can I protect myself?
The best way to avoid zero-day attacks is to follow cyber hygiene best practices:

- Create strong passwords. Use the most complex password allowed, use unique passwords for each platform, and adopt a password manager to simplify password management and ensure secure storage.
- Use multi-factor authentication (MFA). MFA offers an additional layer of protection by requiring two types of credentials, making it harder for hackers to gain access to your device or personal information.

Additional Resources

- Information about known phishing attacks is available from groups such as the Anti-Phishing Working Group.
- CISA Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog