Parental Safeguarding Session

Monday 1st July 2024

Parental Safeguarding Session

Explore some key safeguarding updates around:

- Phishing
- Passwords
- Physical security

Mr McDonald
Assistant Headteacher

Mr Turnbull
Assistant Headteacher

Cyber Safeguarding

Cyber safeguarding refers to the measures and practices put in place to protect digital information, systems, and networks from unauthorized access, damage, disruption, or theft.

It looks at how uses of IT can be kept safe at all times when using the technology.

It encompasses a broad range of activities and strategies designed to secure the integrity, confidentiality, and availability of data and IT resources.

Why Look at Cyber Safeguarding?

Helps to keep students and staff safe.

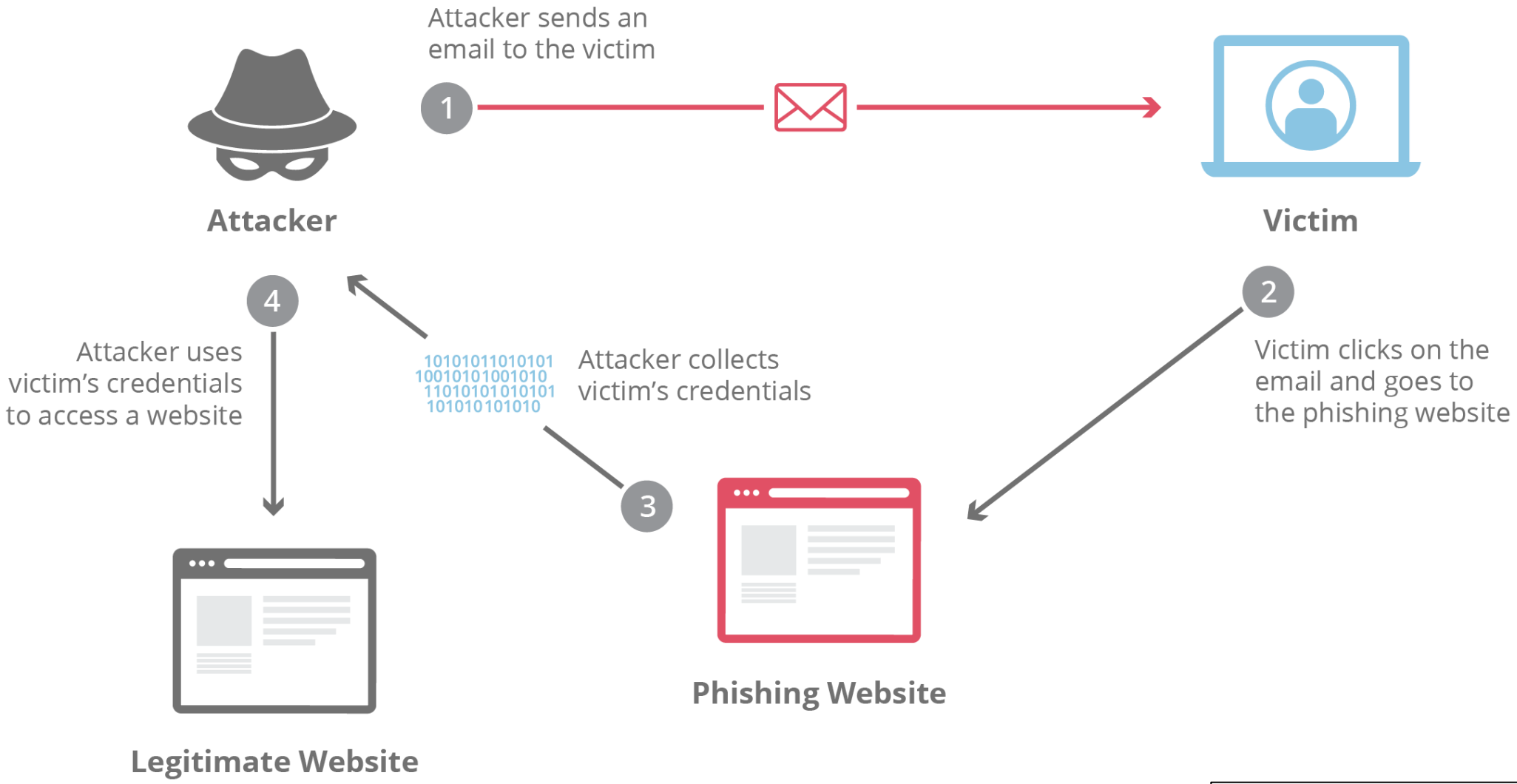
Helps to create a culture where everyone feels comfortable identifying and reporting risk.

Reduces the risk of cyber incidents and attacks.

Makes sure that cyber incidents, attacks and risks are reported quickly to stop them spreading.

Helps everyone understand what acceptable use of digital technology looks like and the importance of cyber security.

Password Phishing



Password Phishing

Protect sensitive information: Passwords safeguard your personal and organizational data from unauthorized access, ensuring confidentiality and integrity.

Prevent unauthorized access: Strong, unique passwords are critical in preventing attackers from easily breaching your accounts and systems.

Phishing Scams

Examples of phishing emails

Example 1: Banking Scam

From: support@bankofengland.com
Subject: Urgent: Verify Your Account Details

Dear Valued Customer,

We have detected unusual activity on your Bank of England account and need you to verify your account details to ensure your account security. Please click the link below to verify your information:

[Verify Account Now](http://fakebankofengland.com)

Failure to verify your details within 24 hours will result in account suspension.

Thank you for your prompt attention to this matter.

Best regards,
Bank of England Security Team

Example 2: Fake Invoice

Dear Customer,

Attached is the invoice for your recent purchase. Please review and process the payment at your earliest convenience.

[Download Invoice](http://maliciouslink.com)

If you have any questions, feel free to contact our support team.

Thank you for your business.

Sincerely,
Invoice Processing Team

Phishing Scams

Key indicators of phishing attempts:

Suspicious Sender Address

Urgent or Threatening Language

Generic Greetings

Poor Grammar and Spelling

Requests for Personal Information

Unusual Requests

Activity

From: support@secure.com
Subject: Urgent! Your account has been compromised

Dear User,

We have detected unusual activity on your account. Please click the link below immediately to verify your identity and secure your account.

[Secure Your Account Now](http://phishingsite.com)

Thank you,
Security Team

The sender's address is suspicious (support@secure.com is generic and not specific to a known company).

The subject line creates a sense of urgency.

The link provided does not match the official domain and redirects to a suspicious URL.

Generic greeting ("Dear User") rather than a personalized greeting.

Keylogging

Keyloggers are malicious programs that secretly record your keystrokes to steal passwords and other sensitive information, posing a significant threat to your online security.

Importance of antivirus software: Using up-to-date antivirus software is crucial for detecting and removing keyloggers and other malware before they can cause harm.

Safe browsing practices: Avoid downloading unknown software, regularly update your system, and practice safe browsing habits to reduce the risk of keyloggers and other cyber threats.

Passwords

Password security is essential for protecting personal and organisational information from unauthorised access.

Cyber threats are constantly evolving, making strong password practices more critical than ever.

A compromised password can lead to data breaches, financial loss, and damage to reputation.

Passwords

Passwords are the primary defence against unauthorised access to our accounts and sensitive information. They protect everything from personal emails and bank accounts to confidential data.

A strong password can prevent cybercriminals from gaining access to your information and using it for malicious purposes.

Weak passwords, on the other hand, are easily cracked using techniques like brute force attacks or social engineering.

Activity

123456	Weak: Too short, common, easily guessable.
Password!	Weak: Common word with a single special character.
C@t$AndD0g$	Strong: Good length, mix of letters, numbers, and special characters.
qwerty	Weak: Common keyboard pattern.
9dx7!H@w2Lz	Strong: Long, complex, mix of characters.
football	Weak: Common word, easily guessable.
Summer2024!	Moderate: Includes a mix of characters but uses a common word and predictable pattern.
Abc123	Weak: Weak: Simple pattern, easily guessable.
!xF7gPq*2	Strong: Mix of characters, less predictable.
letmein	Weak: Common phrase, easily guessable.

Passwords

A strong password is long, complex, and unique. It should include a mix of uppercase and lowercase letters, numbers, and special characters. Avoid using easily guessable information such as names, birthdays, or common words. A good practice is to use passphrases, which are longer and more difficult to crack.

Strong Password

Length: At least 12 characters

Complexity: Mix of uppercase and lowercase letters, numbers, and special characters

Unpredictability: Avoid common words, phrases, and patterns

Uniqueness: Use a unique password for each account

Passwords

Managing multiple strong passwords can be challenging, but several tools and practices can help.

Password managers securely store and generate passwords, making it easier to use unique passwords for each account. Regularly updating your passwords and avoiding the reuse of passwords across different sites is also crucial.

Enable multi-factor authentication (MFA) wherever possible for an added layer of security. Lastly, be cautious of where and how you store your passwords to prevent unauthorised access.

MFA

Enhances Security: MFA requires multiple forms of verification to access an account, such as something you know (password), something you have (phone), and something you are (fingerprint).

Reduces Risk: By adding additional verification steps, MFA significantly reduces the risk of unauthorised access, even if your password is compromised.

Easy to Implement: Most services offer easy-to-setup MFA options. Enable MFA on all your critical accounts to enhance security.

Physical Security

Physically securing devices prevents unauthorized access and potential data theft.

Leaving devices like laptops unlocked and unattended can lead to severe data breaches.

Physical Security

Removable storage media, like USB drives, can easily introduce malware into your system.

These devices can be lost or stolen, leading to potential data breaches. Always using encrypted storage media can mitigate some of these risks but cannot eliminate them completely.

Best Practice

Physical Device Security

Always lock your devices when not in use, even for a short period. Store devices in secure locations when unattended, such as locked rooms, drawers or cabinets.

USBs

Avoid using unverified or unknown USB drives to prevent malware infections. Use encrypted USB drives to protect sensitive data in case the device is lost or stolen. Regularly scan removable storage devices for malware before use.

Activity

Scenario 1

A student leaves their laptop unlocked and unattended on their desk in their classroom while they go to the toilet.

Risk: Unauthorised access to the laptop and sensitive information.
What to do: Always lock your laptop when leaving it unattended, even for a short time. Store it in a secure location if you will be away for an extended period.

Scenario 2

A student uses a USB drive they found in school to transfer files to their computer.

Risk: Potential malware infection from the unverified USB drive.
What to do: Never use unverified or unknown USB drives. Use only trusted and encrypted USB drives and scan them for malware before use.

Parental Safeguarding Briefing
Monday 1st July 2024

Thank you so much for attending this 'Parental Safeguarding Briefing' exploring cybersafeguarding. We really hope that the information shared has been helpful and informative.

If you do have any questions, please feel free to contact school anytime or pose a question in the chat facility. Please ensure questions do not mention any students or staff by name.

If you are ever worried about your child, please contact school. We are here to help.
Thank you for your continued support.