fasthosts ProActive

Oops-proofing your security

Welcome to the first instalment of our “Avoiding Human Error” blog series. In this series, we’ll tackle some of the most common human errors that lead to security breaches and provide you with actionable tips to safeguard your business.

Today, we’re casting a wide net on phishing attacks.

What’s a phishing attack?

Phishing attacks are a form of cybercrime where attackers pose as legitimate institutions, close relations, colleagues, or even friends to lure individuals into providing sensitive data – for example passwords, credit card numbers, or personal information. This is usually done through emails, websites, or messages.

Educate your team

The first line of defence is a well-informed team. Here’s how to educate your staff effectively:

- Regular training – Hold regular cybersecurity training sessions
- Phishing simulations – Run phishing simulations to test your employees. This helps them recognise real threats and understand the consequences
- Clear policies – Establish clear policies on how to handle suspicious emails and report them immediately

What to look out for in an email

Phishing emails can be tricky, but there are common red flags:

- Suspicious sender addresses – Look for email addresses that don’t match the sender’s name or company
- Urgency and threats – Be wary of emails that create a sense of urgency or pressure you into taking action quickly
- Generic greetings – Phishing emails often use generic greetings like “Dear Customer” instead of your name
- Poor grammar and spelling – Legitimate companies usually have professional communications, who would check for mistakes
- Unusual links or attachments – Hover over links to see the URL before clicking
- Requests for money, bank cards, or personal info – Be cautious of emails asking for financial information or personal details, especially if they seem unexpected or out of context

Steps to take if you fall for a phishing attack

So what do you do if you accidentally click that suspicious link or give away some info?

- Disconnect – If you click a malicious link, disconnect your device from the internet to prevent further compromise.
- Change passwords – Immediately change the passwords of any accounts that might be at risk.
- Report the incident – Inform your IT department or security team about the incident. They can help contain the damage.
- Run a security scan – Use antivirus software to scan your device for malware or any unauthorised changes.

Long-term actions

Once the immediate threat is contained, take these steps to make sure your system and data are secure:

- Review security policies – Assess and update your security policies to prevent future attacks
- Monitor accounts – Keep an eye on your accounts for unusual activity
- Educate and update – Share the incident details with your team to prevent similar occurrences
- Adopt cloud infrastructure – Consider services like ours, which regularly scans public-facing IPs to identify potential security vulnerabilities before they become problems. While this won't prevent phishing attacks, it can help mitigate related security risks.

Phishing attacks are a significant threat, but with the right knowledge and proactive measures, you can protect your business from becoming a victim.

Stay tuned for the next post in our "Avoiding Human Error" series, where we'll cover more essential tips to keep your data safe and secure.

If you've got any questions about phishing attacks, or are interested in our services, please get in touch. Give us a call on 0333 111 2000 or book a meeting at a time that suits you.