Don't Take the Bait from Phishing Scammers

In our modern world, the use of emails as a primary form of communication has become the norm. But with this comes the risk of cyberattacks that prey upon you and your employees who use email in increasingly clever ways.

Phishing emails are sent by scammers to try to gain access to basic information from users. Once they have this, they may be able to infiltrate your email, I.T. network, bank account, or other accounts. Even the use of spam filters may not be enough to catch every phishing email that tries to sneak into your inbox. So what can be done to keep your business's information and accounts safe?

Know what to look for. Phishing emails can be very convincing. They might seem to come from friends, family members, coworkers, authorities, or even use familiar logos to appear similar to companies you trust. But if you look closely, there are generally ways to tell if they are legitimate. A few things to keep an eye out for may be:

- Typos and grammar errors
- Incorrect or mismatched email addresses
- Generic signatures
- "Too good to be true" claims or offers of large rewards
- False invoices
- Fear tactics, such as urgent calls to action, suspicious activity, or failed log-in attempts
- Asking you to confirm or fill in personal information

It's important to note that legitimate companies generally have domain emails, won't ask for sensitive information, and don't send unsolicited attachments. Their links will match legitimate URLs, and they won't try to trick you into clicking on anything.[1]

Add extra layers of protection. Make sure to look into the use of anti-virus software and ensure it is up to date. Also, consider the use of multifactor authentication, which requires two or more credentials to log in. If a scammer were to convince an employee to fall for a phishing scam, multifactor authentication can help make it more difficult to successfully get into that employee's accounts.

Back up important data on a regular basis in case the worst were to occur. This is a good practice in general, but can be especially helpful to keep your records and documents in safe standing should the originals be compromised.

Report phishing attempts. If you or your employees have successfully identified a potential phishing email, report the message and delete it from the inbox right away. Most email hosts have an option to report spam and block specific email addresses. If you are questioning the validity of an email, take a moment to read it carefully and look up any keywords or identifying notes that could lead you to make an informed decision. And, if you suspect you clicked on a bad link, take action right away by contacting your information security department.

Phishing emails could put you and your business in danger. When in doubt, be wary of suspicious emails and don't take the bait.

[1] Federal Trade Commission Consumer Information. https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams#recognize