GenAI boosts hackers' trickery: Are you prepared?

With generative artificial intelligence (genAI) tools like ChatGPT, it's easier than ever for hackers to create convincing phishing emails and it's harder than ever for you to spot potential scams. Using genAI, attackers can automate responses in real-time, and launch mass personalized phishing attacks almost instantly, tricking even the most cautious users.

However, there are ways you can fight back against the malicious use of this new technology. Here are three tips for spotting even increasingly sophisticated attacks:

1. **Verify the sender's email address**: Make sure the email address matches the sender's name and is sent from an account that person — or organization — typically uses. If not, it may be a scam.
2. **Beware of requests for sensitive information**: Most organizations will not ask for sensitive information like passwords, social security numbers or financial information through email. If they do, it may be a scam.
3. **Be cautious with unexpected attachments or links**: Stop and think before you click. Ask yourself whether the sender normally sends information in attached files or asks you to click on links in emails. If not, it may be a scam.

Even with genAI making phishing more sophisticated, by following these basic habits you can reduce the chances of scams affecting you and the rest of the Rowan community.

By Sylena Beccles, Information Security Analyst Intern

To mark National Cyber Security Awareness Month this year, Information Resources & Technology will be sharing tips and insight throughout October on how to protect your data — and Rowan's data — when using genAI. For more information on genAI at Rowan, visit go.rowan.edu/genAI. For other online security tips, visit go.rowan.edu/ncsam.

RowanUniversity

201 Mullica Hill Road
Glassboro, NJ 08028
P: 856.256.4000