Gone Phishing!

Understanding Security Scams & Business Complications

Although hackers use sophisticated computer technology to get what they want, in many cases, they rely on simple trickery to gain the access they need to a network. Whether through a tainted attachment, a phony email or a fraudulent phone call, cybercriminals often use subterfuge to break into a business's network. Here are common types of security scams that businesses can encounter — and some tricks they can use to avoid them.

Business Email Compromise

When a cybercriminal gains access to a single email account for a high-ranking company official, he or she can use that to send fraudulent emails requesting unauthorized financial transactions.

How to Protect Yourself

- Require multiple authentications for any financial transactions requested through email.
- Require everyone in the company to update their passwords on a regular basis.

Ransomware

Hackers can insert malicious code into a company's network that will restrict access unless the company pays the hackers a ransom.

FILES ARE ENCRYPT
otos, documents and other impo
ve been encrypted with unique
nerated for this computer.
NEXT

How to Protect Yourself

- Always ensure your network's security is up to date.
- Make regular backups of sensitive information in the event that ransomware locks you out of your system.

Phishing

Fraudulent emails can fool employees into giving out sensitive information, allowing hackers and cybercriminals to access company networks.

How to Protect Yourself

- Educate employees about phishing scams and show them how to spot them.
- Use an email security platform that can block suspicious spam emails before they reach employees' inboxes.

Dynamic Data Exchange Attacks

Malicious code can be hidden inside of files such as PDFs and Word documents that are shared via email. When these files are opened, the code is activated and installs itself on the network, opening the door for hackers to steal information.

How to Protect Yourself

- Make sure employees understand the risks of opening documents they didn't request or weren't expecting.
- Keep security protocols up to date and make sure they include email filtering to protect against spam.

Voice Phishing

This is an analog version of the phishing scam. Criminals in these types of scams impersonate representatives from financial institutions and trick employees into giving out PINs and other sensitive information.

How to Protect Yourself

- Educate employees about phishing scams and make sure they know when to be suspicious.
- Use VOIP security systems that will help prevent suspicious phone numbers from connecting to your network.

access one
www.accessoneinc.com