skött-i.t.
TECHNOLOGY GROUP

PHISHING SCAMS

Protect Your Business From Phishing Attacks

HOW IT HAPPENS

You've probably seen it happen before, a client or vendor asks you to click on a link to download a file you requested. Do you click on it? What if the request is from your boss and he's asking for his lost password? In most cases, the answer is No – this is one of the most common types of phishing attacks.

You get an email or text

It appears to be from someone you know, and asks you to click on a link, or forward a password or your bank account information. Sometimes it can appear to be from your boss or a manager.

It's urgent

The message pressures you to do something immediately — for some urgent matter. Many attempts are based around wiring funds, changing passwords, COVID-19 or some other national crisis.

It appears real

The message appears very real, but can use fake email addresses – sometimes off by just one letter. Scammers will use well known company names and pretend to be someone you know.

What happens next

By clicking on a link, you can unintentionally install a virus, malware, or ransomware that locks you out of your data. This can infect other computers on the network. If you shared any passwords with other co-workers, the scammers now have access to these accounts.

skött-i.t. TECHNOLOGY GROUP

PHISHING SCAMS

WHAT YOU CAN DO ——

Never click and share any sensitive business information:

Make sure it's legitimate
Try to identify the website or phone number for the business or person pretending to be sending the email. You want to be certain you are contacting the actual company and not downloading malware or virus – or possibly talking to a scammer.

If you're unsure – ask someone
Asking a co-worker can help determine if the request is real or a phishing scam. You're probably not the first person in the company to get a scam email.

Verify with verbal communication
Never trust an email pushing for any kind of request. Call the client, vendor or employee who sent the email. Get verbal confirmation that they really need the information. This can't be stressed enough – especially concerning any kind of money transfer.

PROTECT YOUR BUSINESS -

Keep your security up to date
Make sure your operating system is up to date. Use additional protection such as two-factor authentication and antivirus/malware software. Mobile devices are just as vulnerable.

Keep good backups
Having a good data backup is critical for recovery if you are compromised. Keep backups off the network so they can't be affected. Data backups should be a regular part of your daily IT strategy.

Deploy a safety net
Make sure your email provider is utilizing a proven authentication method. This verifies that email comes from who it claims to be from. Common standards are SPF, DKIM, and DMARC.

Alert your staff
Share this with your staff. Phishing scammers change their methods often, so update your tips for identifying scams during your regular training.

WHAT IF YOU ENCOUNTER A PHISHING SCAM –

Immediately follow your company's protocols
These may include notifying specific people in your organization or support providers that help you with IT.

Contact staff
Discuss with staff and compare your experience. Phishing scams often happen to others in the company.

Control any damage
Disconnect the compromised computer from the network, immediately change any affected passwords.

Contact your customers
If your information was compromised, notify any affected party or client, as they could be at risk as well.

skött-i.t. TECHNOLOGY GROUP

SECURITY CHECKLIST

How To Protect Your Business From A Cyber Attack!

Here are a few important steps you can take to prevent a cyber attack.
Give your business IT a quick audit to see if you are protected against most known threats.

- ☐ **Assess your Security**
  Assess your security to establish a standard baseline for your business. Eliminate all vulnerabilities.

- ☐ **Phishing Attack Security Awareness**
  Train staff on email phishing scams. This should be done often and ongoing since phishing attacks are becoming more sophisticated.

- ☐ **Spam and Phishing Email**
  Review your email security. Use a reliable vendor for mail hosting, tighten spam measures, employee authentication standards such as SPF, DKIM, and DMARC.

- ☐ **Utilize Two-Factor Authentication**
  Use two-factor authentication where possible. This is used for email, banking websites, social media and even server solutions. This second layer of security ensures your account is protected even if your password is stolen.

- ☐ **Check your Passwords**
  Apply Strict Password Policies. Use a password manger such as 1Password to store all your passwords. Set computer screen timeouts to require a password on wake.

- ☐ **Advanced Endpoint Detection & Response**
  All computers should run virus and malware protection. Today's advanced software can protect against file-less and script based threats and even mitigate some ransomeware attacks.

- ☐ **Operating System Updates**
  Make sure your computer OS and apps are up to date. This ensures you have the latest security bugs fixed. Don't forget firmware updates for your server and firewall as well.

- ☐ **Backups**
  Backup, backup, backup – this can't be stressed enough. Backup your data locally and off-site. Backups should be regularly tested to ensure recoverability. Make sure you frequently test that all backups are working properly.

- ☐ **Firewall**
  All access through your firewall should be denied except for services that are required to run your business operation. If available, turn on intrusion detection and intrusion prevention features.

- ☐ **Mobile Device Security**
  Limit public WiFi – hackers specifically target unsuspected users on public WiFi networks that look safe, but they are really vulnerable to attacks. Use a Mobile Device Management (MDM) solution for better security and remote wipe capabilities.

- ☐ **Encryption**
  Encrypt files where possible. Today's computers can easily provide disk encryption which can ensure your data is safe even if the computer is lost or stolen.

skött-it technology group

We provide all types of security solutions for the small and medium size business.
Give us a call today for a free security audit and let us help you secure your business data.

skött-it technology group 407.259.2900 info@skottit.com www.skottit.com