2021

Common Threats

Kevin Mitnick, Chief Hacking Officer at KnowBe4, breaks down two of the latest **social engineering** attack strategies bad actors are using against you and your organization and provides steps you can take to stay safe.

SINGLE SIGN-ON PHISHING ATTACKS

Many organizations use single sign-on (SSO) services, like Okta and OneLogin, to streamline user access to their applications. Although convenient, if hackers gain access to your SSO information, they can access all of the services that you can.

How do hackers achieve this? By sending a **phishing** email stating you need to update a compromised password for your SSO application. While doing that, you will need to enter the generated **2FA** code, which usually helps secure your account.

Unfortunately, you actually granted them access to your SSO and your organization's resources.

You have to think about the nature of the email. Ask yourself, what is the sender asking you to do? Is this request in the normal course of business, and have you been asked to do this before? Even if you're cautious and hover over the link, you still need to stop, look, and think because it might be deceptive.

PASSWORD MANAGER PHISHING ATTACK

People use password managers to auto-generate strong and unique passwords and then store them for easy access later. But a centralized access point to your stored **credentials** is a gold mine for bad actors.

How do hackers target password managers? They send a phishing email urgently indicating you have to update your master password. The real trick is they tell you that you have to accept an authentication request sent to your email to secure all of your other credentials.

Unfortunately, when you confirmed the authentication request, you granted the bad actor access to your password manager. They can now download your password manager's contents to their device and have access to all your accounts.

That's why it's so important to stop, look, and think whenever you're asked to enter account credentials, provide 2FA codes, or reset password manager credentials.

IMPORTANT TERMS

Becoming familiar with the language hackers use is an important first step to understanding how they try to trick you.

SOCIAL ENGINEERING

The act of manipulating people into performing actions or divulging confidential information.

PHISHING

The process of attempting to trick you into giving out sensitive information or taking potentially dangerous actions by using email to impersonate contacts or organizations you trust.

TWO-FACTOR AUTHENTICATION (2FA)

A method of confirming or authenticating an individual's identity through the use of two or more verification steps, such as entering your username and password and then receiving a text.

CREDENTIALS

The information that a user enters to prove that they are authorized to access a particular device or resource.

KnowBe4