Awareness

Your First Steps Towards Digital Security

dPhish

Introduction

Get ready to uncover the secrets of staying safe in our digital world! In this book, we break down the essentials of information security simply and engagingly. Discover how cyber attackers can sneak into our lives, snatch our data, and invade our privacy. But fear not — we've got your back! Learn the ropes of preventing and defending against these digital threats.

In a world where we're glued to our phones and computers, even non-techies are vulnerable. Cyber attackers are upping their game, especially with phishing attacks on the rise.
Wondering where to start to protect your data and privacy? We've got you covered! Dive into topics like secure online banking, savvy online shopping, avoiding social media traps, and even tips for guiding your kids through the digital jungle. Let's embark on this journey together to fortify your digital fortress!

Content:

1 Financial Fraud

2 Social Media Fraud

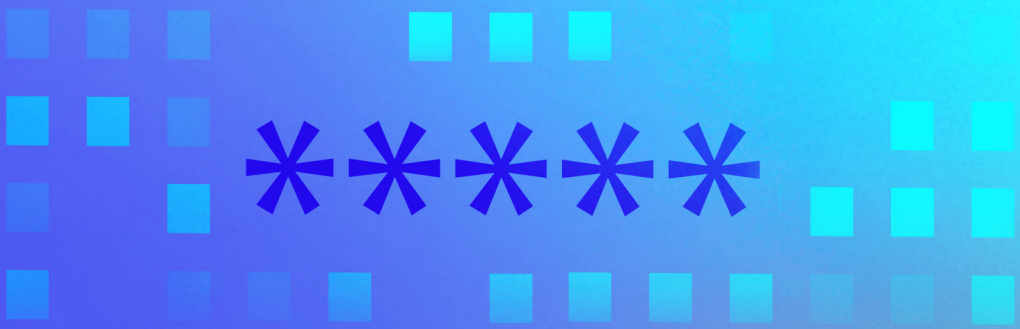
3 Online Shopping Safety

4 Children's Awareness

Financial Fraud:

When you buy stuff online and use your **credit/debit card**, they usually ask for important details like the **16-digit card number**, expiry date, CVV (those 3 digits on the back), and your name as it appears on the card.

But sometimes, your info can be at risk. That's why many banks add extra protection. They send a special code (**6 digits**) to your phone via text or another secure way. This code is like a secret handshake, making sure it's you are making the payment.



Seems easy and safe, doesn't it? Now, **imagine this scenario:**

You receive a text from your trusted bank with a 6-digit code. Right after, you get a call from an unknown number with a friendly voice claiming to be from the bank. They urgently ask for those numbers, stating it's crucial to prevent issues like locking your account or stopping an attack.

Here's the deal: NEVER share those numbers in such a situation. No legitimate bank will ask for them because it's against the rules and giving them away could mean handing over your hard-earned money to a scammer.

The OTP for the online purchase of card number 5699 is 98617, and it will expire in 10 minutes. Please do not share this code with anyone for any reason.

كلمة المرور لمرة واحدة لشراء البطاقة رقم 1234 عبر الإنترنت هي 986179. وستنتهي صلاحيتها خلال 10 دقائق. يرجى عدم مشاركة هذا الرمز مع أي شخص لأي سبب من الأسباب.

If you ever find yourself in this situation, take these steps:

Call your bank right away, ask for a card freeze, and get a new card.

Change your online banking passwords and PINs connected to the card for extra security.

Keep an eye on your bank statements regularly to catch and report any transactions you didn't authorize.

Now, let's talk about another sneaky fraud tactic! You might get a message claiming there's an attack, urging you to click a link ASAP.

Here's the deal:

1

Just because you got an SMS from someone posing as your bank doesn't mean your account is in danger. Stay calm.

2

If you get such a message, reach out to your bank directly and avoid clicking that link at all costs.

3

A legitimate bank will never ask you to click a link to fix issues like these. Stay cautious and keep your money safe!

> *Urgent: Your account security is compromised. Immediate action required. Click the link below to verify your idedtity and prevent unauthorized access.*

الاحتيال عبر مواقع التواصل الاجتماعي

تعد وسائل التواصل الاجتماعي مكانًا يسيرا لممارسة الاحتيال، حيث يمكننا جميعا مشاركة أفضل لحظاتنا، والتواصل مع الأصدقاء والعائلة والضحك معًا، لكن تعلم كيف تسير الأمور. هناك دائمًا **"لكن"!**

تخيل هذا: أنت تقضي يومك فحسب، وتتصفح رسائل الوسائط الاجتماعية الخاصة بك، فجاة تصلك رسالة مثل هذه :

عرض لفترة محدودة : احصل على تذكرة عمرة مجانية! التصرف بسرعة!

عزيزي مصطفى،

لا تفوت! لديك فرصة للحصول على تذكرة عمرة مجانية لفترة محدودة. قم بتأمين مكانك الآن. https:\\bit.ly/dsfVdshf

عاجل : مسابقة لفترة محدودة مع فرصة للفوز بجائزة!

يسعدنا أن نعلن عن فرصة حصرية لك! تصرفوا بسرعة، لأن الوقت ينفد للمشاركة في مسابقتنا المثيرة مع فرصة الفوز بجوائز مذهلة، بما في ذلك أحدث الهواتف الذكية! **أبرز مميزات الجائزة:**

-الهواتف الذكية الجديدة - خصومات وعروض حصرية - قسائم هدايا مثيرة

لا تفوت فرصتك في الحصول على هذه المكافآت الرائعة.

هذه المسابقة مفتوحة لفترة محدودة فقط، وقد تؤدي مشاركتك إلى تحقيق مكاسب كبيرة! للدخول وتأمين فرصتك في هذه الجوائز المذهلة، انقر على الرابط أدناه الآن :https.\\bit.ly أسرع، فهذه الفرصة لن تدوم طويلًا! تصرف الآن، وقد تكون الفائز المحظوظ التالي.

تبدو هذه الهدايا جميلة جدًا، أليس كذلك؟ ولكن لنكن واقعيين.

لماذا يقوم شخص ما بالتبرع بمثل هذه الأشياء القيمة مجانًا لأشخاص عشوائيين؟

أولاً وقبل كل شيء، لا ترد على الرسالة أو تتفاعل مع المرسل بأي شكل من الأشكال. تجنب الضغط على أي رابط أو تنزيل أي ملف من الرسالة. فإن فعلت؛ فإن هذا سيؤدي إلى اختراق خصوصيتك و تحميل برمجيات خبيثة على هاتفك او حاسوبك.

ما سبق هو واحد من أشهر طرق الاحتيال المنتشرة عبر مواقع التواصل الاجتماعي، وهناك طرق أخرى كثيرة تشاركه نفس الصفات. رسائل جميلة بشكل غير واقعي، تطلب منك بياناتك أو الضغط على رابط، أو تحميل ملف، أو يقوم باستدراجك لمحادثة أطول ثم يقوم بسرقتك!

هناك أيضا من يستغل رغبتنا في الحصول على وظيفة من المنزل من خلال الانترنت، فهذا شيء رائع لأغلبنا! ولكن – من تجاربنا –أغلب هذه الرسائل مزيفة، فلا ترد عليها إن لم تأتى من شخص موثوق تعرفه جيدا.

احمي نفسك اثناء التسوق عبر الانترنت

يجب أن أعترف أنني من محبي التسوق عبر الإنترنت! فإنه يغيّر قواعد اللعبة في عالمنا سريع الخطى، حيث توفير الراحة بالحصول على ما تحتاجه – فقط – ببضع نقرات!

Imagine you're waiting for a package, and you get an email like this:

> **The status of your shippment has changed:**
>
> We made an attempt to deliver your package today, but unfortunately, you werent available.
> ----shippment details----
> Reference number: SJFSJFNSLMF
> Tracking number: GH45OJKLSDN
>
> We sincerely apologize for any inconvenience caused. To reschedule your delivery and provide updated address, kindly click on the following link:
> https:\\bit.ly\dgsf78s

Sounds familiar, right? But it can be tricky. Sometimes, clicking the link is not safe. Here's how to tell if it's real or fake:

1. Check the company's name. If you expect an email from Amazon but it's from Vidix, it's probably fake.
2. Read the email carefully to make sure it's really from the company you were expecting.
3. If you clicked the link and a file downloads, delete it right away. Don't open it, and never enter your username or password if asked.
4. Track your package directly on the official website instead of using links in emails.

Emphasize the importance of talking to a trusted adult if they encounter something online that makes them feel uneasy or uncomfortable.

Make sure they understand that updating their apps and games is like adding extra armor; it fixes bugs and enhances security.

Extreme caution is essential. Your children should always check with you before sharing sensitive or personal information online.

dPhish Overview:

dPhish, established in 2022, As an Arabic Company, operates across Arab and international markets, specializing in anti-phishing solutions and enhancing employee security awareness. Aspires to become a pioneering presence in both Arab and foreign markets, distinguishing itself through a range of unique benefits.

Book Overview:

Driven by our commitment to spreading security awareness throughout society and recognizing its impact on every individual, we conceived the idea of a concise guidebook. This guide aims to elevate security awareness within each household, making it accessible for every family member. Our motivation stems from a desire to contribute positively to the society we proudly belong to.

The book covers various topics in information security tailored for non-tech individuals, serving as a reliable guide for safe internet browsing. We trust you will find it valuable and welcome your feedback on our company's website. Join us on a journey to fortify protection against digital deception.

Contact Us

Awareness.booklet@dphish.com

sales@dphish.com

dphish.com/contacts

Egypt, Cairo Namaa Building 5th floor, Emtedad Ramses

USA, Las Vegas, Nevada 304 S.Jones Blvd #817